PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 30 August 2000 (30.08.00)	
International application No. PCT/FI99/01036	**Applicant's or agent's file reference** 12714S
International filing date (day/month/year) 15 December 1999 (15.12.99)	**Priority date** (day/month/year) 16 December 1998 (16.12.98)
Applicant VATANEN, Harri	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

05 July 2000 (05.07.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer F. Baechler
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

Copy for the Elected Office (EO/US)

PCT/FI99/01036

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

From the INTERNATIONAL BUREAU

To:

PAPULA OY
P.O. Box 981 (Fredrikinkatu 61 A)
FIN-00101 Helsinki
FINLANDE

Date of mailing (day/month/year)
30 August 2000 (30.08.00)

Applicant's or agent's file reference
12714S

IMPORTANT NOTIFICATION

International application No.
PCT/FI99/01036

International filing date (day/month/year)
15 December 1999 (15.12.99)

1. The following indications appeared on record concerning:

[X] the applicant [X] the inventor [ ] the agent [ ] the common representative

Name and Address
VATANEN, Harri
40 Alma Road
Windsor, Berkshire SL4 3HJ
United Kingdom

State of Nationality: FI
State of Residence: GB
Telephone No.:
Facsimile No.:
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address
VATANEN, Harri
2 Rushmere Place
Englefield Green
Surrey TW20 0NN
United Kingdom

State of Nationality: FI
State of Residence: GB
Telephone No.:
Facsimile No.:
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[X] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
F. Baechler

Telephone No.: (41-22) 338.83.38

Form PCT/IB/306 (March 1994)

003496419

F ENT COOPERATION TREA

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

PAPULA OY
P.O. Box 981 (Fredrikinkatu 61 A)
FIN-00101 Helsinki
FINLANDE

Date of mailing (day/month/year) 30 August 2000 (30.08.00)	
Applicant's or agent's file reference 12714S	**IMPORTANT NOTIFICATION**
International application No. PCT/FI99/01036	**International filing date** (day/month/year) 15 December 1999 (15.12.99)

1. The following indications appeared on record concerning:

[X] the applicant [ ] the inventor [ ] the agent [ ] the common representative

Name and Address	State of Nationality	State of Residence
SONERA SMARTTRUST OY Teollisuuskatu 15 FIN-00510 Helsinki Finland	FI	FI
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address	State of Nationality	State of Residence
SONERA SMARTTRUST OY c/o Sonera Oyj P.O. Box 106 FIN-00051 Sonera Finland	FI	FI
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[X] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer F. Baechler
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

To:

PAPULA OY
P.O. Box 981 (Fredrikinkatu 61 A)
FIN-00101 Helsinki
FINLANDE

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

Date of mailing (day/month/year)
19 July 2000 (19.07.00)

Applicant's or agent's file reference
12714S

IMPORTANT NOTIFICATION

International application No.
PCT/FI99/01036

International filing date (day/month/year)
15 December 1999 (15.12.99)

1. The following indications appeared on record concerning:

[X] the applicant [ ] the inventor [ ] the agent [ ] the common representative

Name and Address
SONERA OYJ
Teollisuuskatu 15
FIN-00510 Helsinki
Finland

State of Nationality: FI
State of Residence: FI
Telephone No.:
Facsimile No.:
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [X] the name [ ] the address [ ] the nationality [ ] the residence

Name and Address
SONERA SMARTTRUST OY
Teollisuuskatu 15
FIN-00510 Helsinki
Finland

State of Nationality: FI
State of Residence: FI
Telephone No.:
Facsimile No.:
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[X] the designated Offices concerned
[ ] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
Beate Giffo-Schmitt

Telephone No.: (41-22) 338.83.38

Copy for the designated Office (DO/US)

PCT/FI99/01036

F ENT COOPERATION TREA

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

PAPULA OY
P.O. Box 981 (Fredrikinkatu 61 A)
FIN-00101 Helsinki
FINLANDE

Date of mailing (day/month/year)
29 June 2000 (29.06.00)

Applicant's or agent's file reference
12714S

IMPORTANT NOTIFICATION

International application No.
PCT/FI99/01036

International filing date (day/month/year)
15 December 1999 (15.12.99)

1. The following indications appeared on record concerning:

[ ] the applicant [ ] the inventor [X] the agent [ ] the common representative

Name and Address
PAPULA REIN LAHTELA OY
P.O. Box 981 (Fredrikinkatu 61 A)
FIN-00101 Helsinki
Finland

State of Nationality

State of Residence

Telephone No.
+358 9 3480 060

Facsimile No.
+358 9 3480 0630

Teleprinter No.

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [X] the name [ ] the address [ ] the nationality [ ] the residence

Name and Address
PAPULA OY
P.O. Box 981 (Fredrikinkatu 61 A)
FIN-00101 Helsinki
Finland

State of Nationality

State of Residence

Telephone No.
+358 9 3480 060

Facsimile No.
+358 9 3480 0630

Teleprinter No.

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[X] the designated Offices concerned
[ ] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
Jocelyne Rey-Millet

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

RECD 27 MAR 2001
WIPO PCT

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 12714S	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FI99/01036	International filing date *(day month year)* 15.12.1999	Priority date *(day month year)* 16.12.1998
International Patent Classification (IPC) or national classification and IPC7 H04L 9/32		
Applicant Sonera Smarttrust OY et al		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 4 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
05.07.2000	20.03.2001
Name and mailing address of the IPEA/SE Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Facsimile No. 08-667 72 88	Authorized officer Rune Bengtsson /OGU Telephone No. 08-782 25 00

Form PCT/IPEA/409 (cover sheet) (January 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

[redacted]ational application No.
PCT/FI99/01036

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:
pages 1-13 , as originally filed
pages _____ , filed with the demand
pages _____ , filed with the letter of _____

☒ the claims:
pages _____ , as originally filed
pages _____ , as amended (together with any statement) under article 19
pages _____ , filed with the demand
pages 14-17 , filed with the letter of 24.01.2001

☒ the drawings:
pages 1-4 , as originally filed
pages _____ , filed with the demand
pages _____ , filed with the letter of _____

☐ the sequence listing part of the description:
pages _____ , as originally filed
pages _____ , filed with the demand
pages _____ , filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language English which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☒ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheet/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2 (c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item I and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

[redacted]ational application No.
PCT/FI00/01036

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-14	YES
	Claims		NO
Inventive step (IS)	Claims	1-14	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-14	YES
	Claims		NO

2. Citations and explanations (Rule 70.7)

D1: EP 689316 A2
D2: US 5018196 A

The invention relates to a method and a system for digitally signing an electronic form in a secure manner by means of a mobile station. The most significant feature is that a hash code is used for verifying the authenticity of the signed and transferred material. Hash code in the signed material is compared with hash code computed from the material before signing.

In amended claims 1 and 10 the differences between the invention and the state-of-the-art technology as represented by D1 and D2 are clearly defined.

Therefore, the requirements of novelty and inventive step are now considered fulfilled.

Also the requirement of industrial applicability is fulfilled.

PCT/ FI 99/ 01036
24 -01- 2001

CLAIMS

1. Method for digitally signing an electronic form in a secure manner by means of a mobile station, said method comprising the steps of

transferring the material to be signed, which comprises the form, its identifier, shared information, and/or essential information added to it, to the mobile station, characterized in that

a first hash code (H1) is computed from the material to be signed;

the first hash code is added to the material, to be transferred to the mobile station;

the material transferred to the mobile station is signed digitally by means of the mobile station; and

the authenticity of the signed and transferred material is verified by comparing the signed hash code with the first hash code computed from the material before signature.

2. Method as defined in claim 1, characterized in that

the material transferred to the mobile station for signature is transferred to a second party; and

the signed material is transferred to the second party, whereupon the second party verifies the authenticity of the signature.

3. Method as defined in claim 1 or 2, characterized in that

the material is encrypted before being transferred between the mobile station and the second party; and

the encrypted material is decrypted before any treatment of the material, such as signature and verification of authenticity.

4. Method as defined in any one of the preceding claims 1 - 3, characterized in that

the form is generated using a pre-agreed form template provided with an identifier, the essential information being filled in in the form template before it is transferred to the mobile station.

5. Method as defined in any one of the preceding claims 1 - 4, characterized in that

the hash code is generated using a hash function.

6. Method as defined in any one of the preceding claims 1 - 5, characterized in that

the signature and/or encryption of the message is implemented using a public and private key method.

7. Method as defined in any one of the preceding claims 1 - 6, characterized in that

the material and/or part of it is presented in the mobile station before the material is signed.

8. Method as defined in any one of the preceding claims 1 - 7, characterized in that

the mobile station is started in signature mode before the transfer of the material into the mobile station.

9. Method as defined in any one of the preceding claims 1 - 8, characterized in that

the material is stamped with a time stamp; and

the transaction of signature of the material is filed after the signature has been authenticated.

10. System for digitally signing an electronic form in a secure manner by means of a mobile station (MS), said system comprising

a payment machine (2);

means (3) connected to the payment machine for the generation of the material to be signed, said material comprising a form, its identifier, shared data, and/or essential information added to it; and

means (4) connected to the payment machine for the transfer of the material into the mobile station (MS), characterized in that

the payment machine comprises means (5) for computing a first hash code (H1) from the material to be signed;

the mobile station comprises signing means (6) for the signing of the material transferred into it; and

the payment machine comprises means (7) for verifying the authenticity of the signed and transferred material by comparing s signed hash code ($H1_{ds}$) with the hash code (H1) computed from the material before signature.

11. System as defined in claim 10, characterized in that the system comprises

a server (8) connected to the payment machine (2) and the mobile station (MS) and controlled by a third party; and

the mobile station comprises means for encrypting the signed material.

12. System as defined in claim 10 or 11, characterized in that the server (8) comprises

means (9) for the verification of authenticity of the digital signature.

13. System as defined in any one of the preceding claims 10 - 12, characterized in that the mobile station comprises

means (10) for presenting the material and/or part of it in the mobile station before the signing of the material.

14. System as defined in any one of the preceding claims 10 - 13, characterized in that the server (8) comprises

means (11) for stamping the material with a time stamp; and

means (12) for filing the transaction of signing of the material after the signature has been authenticated.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/32 — A1

(11) International Publication Number: **WO 00/39958**

(43) International Publication Date: 6 July 2000 (06.07.00)

(21) International Application Number: PCT/FI99/01036

(22) International Filing Date: 15 December 1999 (15.12.99)

(30) Priority Data:
982728 16 December 1998 (16.12.98) FI

(71) Applicant *(for all designated States except US)*: SONERA OYJ [FI/FI]; Teollisuuskatu 15, FIN–00510 Helsinki (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: VATANEN, Harri [FI/GB]; 40 Alma Road, Windsor, Berkshire SL4 3HJ (GB).

(74) Agent: PAPULA REIN LAHTELA OY; P.O. Box 981 (Fredrikinkatu 61 A), FIN–00101 Helsinki (FI).

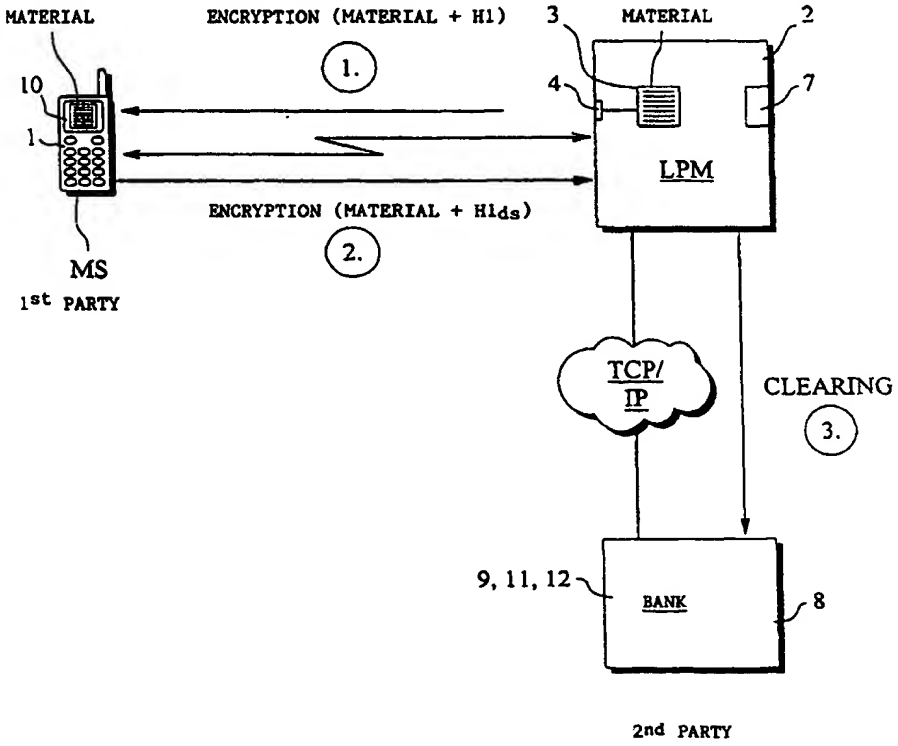
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
In English translation (filed in Finnish).

(54) Title: METHOD AND SYSTEM FOR IMPLEMENTING A DIGITAL SIGNATURE

(57) Abstract

Method for digitally signing an electronic form in a secure manner by means of a mobile station. In the method, the material to be signed, which comprises a form, its identifier, shared information, and/or essential information added to it, is transferred to the mobile station, a first hash code (H1) is computed from the material to be signed, the hash code is added to the material for transfer into the mobile station, the material transferred into the mobile station is signed digitally by means of the mobile station and the authenticity of the signed and transferred material is verified by comparing the signed hash code with the hash code computed from the material before the signature. Thanks to the invention, a mobile station can be safely used for digital signature in various applications.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND SYSTEM FOR IMPLEMENTING A DIGITAL SIGNATURE

The present invention relates to telecommunication systems and to a technique for signing and encrypting digital information. In particular, the invention relates to a system which makes it possible to sign an electronic form or other electronic information and to verify the authenticity of the signature and the signatory.

BACKGROUND OF THE INVENTION

In prior art, the use of a digital mobile station, e.g. a mobile station in the GSM system (Global System for Mobile communications, GSM), for commercial transactions, such as paying a bill or making a payment by electronic means, is known. Patent application US 5,221,838 presents a device which can be used for making a payment. The specification describes an electronic payment system in which a terminal device capable of wired and/or wireless data transfer is used as a payment terminal. The terminal device according to the specification comprises a card reader, a keypad, a bar code reader for the input of information and a display unit for presenting the payment information.

Patent specification WO 94/11849 discloses a method for the utilization of telecommunication services and execution of payment transactions via a mobile telephone system. The specification describes a system comprising a terminal device which communicates over a telecommunication system with a service provider's mainframe computer containing the service provider's payment system. The terminal device used in a mobile telephone network, i.e. the mobile station, can be provided with a subscriber identity module comprising subscriber information for the identification of the subscriber and for the encryption of telecommuni-

cation. The information can be read into the terminal device so that it can be used in mobile stations. The specification mentions the GSM system as an example, in which a SIM card (Subscriber Identity Module, SIM) is used as a subscriber identification unit.

In the system according to WO 94/11849, the mobile station communicates with a base station comprised in the mobile telephone network. According to the specification, a connection is further established with the payment system, and the amount to be paid as well as the data required for the identification of the subscriber are transmitted into the payment system. In the bank service described in the specification, the client places a service card given by the bank and containing a SIM unit into a terminal device used in the GSM network. In telephone based bank service, the terminal device may be a GSM mobile station consistent with the standard. Using the method described in the specification, a wireless telecommunication connection can be used for making payments and/or paying bills or implementing other bank or cash services.

The problem with the above-mentioned solutions is that they do not involve any consideration of reliability of the payment from the payer's and the payee's point of view. When a mobile station is used for making a payment, it is important that both the payer and the payee can trust the system. The payer must know exactly what he is paying for, how much he is paying, to whom he is paying, how he is paying etc. The payee must also know exactly who is paying for what and how much etc.

As is well known, transmitting information in electronic form from one place to another is easy. However, it is more difficult to make sure that the information transmitted remains unchanged during the transmission and that e.g. the information presented

on the display of a mobile telephone is transmitted in exactly the same form and unchanged to the receiver.

A previously known practice is to use a hash code, which is a data field formed and computed from the information to be transmitted. The hash code is generally computed using an algorithm which is a one-way function, in other words, the hash code can not be deciphered so as to reveal the information from which it has been generated. An algorithm that may be used for this purpose is SHA-1 (Secure Hash Algorithm).

A digital signature, which is considered as a general requirement in electronic payment, is used to verify the integrity of the material transmitted and the origin of the sender. A digital signature is generated by encrypting a hash code computed from the material to be transmitted, using the sender's secret key. As nobody else knows the sender's secret key, the receiver decrypting the encrypted material can be assured that the material is unchanged and generated by the sender. An example of an algorithm used in digital signatures is the RSA encryption algorithm, which is an encryption system based on a private key and a public key and which is also used for the encryption of messages.

OBJECT OF THE INVENTION

The object of the present invention is to eliminate the problems referred to above. A specific object of the invention is to disclose a new type of method and system for the signing of a form or corresponding information by means of a mobile station. In this context, `form' may refer to many types of message, dispatch or information structure with various contents. The form may consist of object type or software object type information which can be processed in electronic form.

A further object of the invention is to disclose a simple method for implementing commercial transactions, such as paying a bill and transacting business with a bank, using a mobile station, a method that is easy to implement with present technology.

SUBJECT OF THE INVENTION

The invention concerns a method for signing an electronic form as defined above with a digital signature in a secure manner using a mobile station or some other equivalent and comparable device. In the method, the material to be signed, which may comprise at least the form, its identifier, shared data, and/or essential information added to the form, is transferred into the mobile station. The material to be signed can also be generated from an identifier of the form and essential information associated with the form; for instance, in the case of a bank transfer form, the material to be signed may be generated from the identifier of the bank transfer form and the data in the essential fields in it, such as the payer, payee and amount fields.

According to the invention, from the material to be signed, a first hash code is computed, preferably before the material is transferred into the mobile station. The hash code is added to the material, to be transferred with it, thus allowing the hash code to be used as an aid in verification. After the material has been transferred into the mobile station, it is signed in the mobile station and, further according to the invention, the authenticity and conformity of the signed and transferred material are verified by comparing the signed hash code with the hash code computed from the material before signature. The signature can also be accomplished by signing both the essential information and the hash code, in which case it will even ensure that the material signed via the

mobile station corresponds to the material transferred for signature.

In the case of certain types of application, such as payment applications, the material transferred into the mobile station can also be transferred to a second party, e.g. a bank, which can compute a hash code from the material received. The material signed in the mobile station can further be encrypted and the encrypted and signed material can be transferred from the mobile station to the second party as well. The second party decrypts the encrypted information, verifies the signature, computes a second hash code from the material received from the mobile station and compares it with the first hash code computed from the original material. If the second party accepts the digital signature and if the first and second hash codes correspond to each other, then the bank will accept the signature made via the mobile station. After the bank has accepted the signature, it can put a time stamp in the signed and encrypted material and file the transaction of signature of the material.

The case described above is a procedure in which a client of a bank signs a form received from the bank. The client or mobile station user may communicate locally with an automated payment machine or equivalent, in which case the payment machine transmits to the client a form for payment and approval. In this case, the client exchanges messages with the payment machine locally and the payment machine transmits the digital signature data further. However, the payment machine can infer from the communication it is transmitting that the client has accepted the service and payment form offered to it. The machine can serve the client locally in a manner desired and paid for by the client, without necessarily waiting for the bank's approval of it. In practice, the situation corresponds to the normal practice where e.g. a customer at a

shop's cash machine pays for products or services with a cash card and the shop provides them to the customer without verifying the authenticity of the payment by contacting the bank.

The material can also be encrypted before being transferred into the mobile station, in which case the material has to be decrypted in the mobile station before signature. This expedient can be used to ensure that only the desired mobile station will receive the material to be transferred and to guarantee the security of the information.

The form can be generated using a pre-agreed form overlay, message structure or any other information structure, provided with an identifier, in which pre-agreed essential information is filled in before the form is transferred into the mobile station. The hash code can be computed using e.g. a hash function. For the signature and/or encryption of the message and/or form, a public and private key method can be used.

In a preferred embodiment of the invention, the material and/or part of it is presented in the mobile station prior to the signing of the material. For example, the payee, payer and reference information and the amount payable may be presented. It is also possible to require that the mobile station be started in signature mode before the transfer of the material into it. In practice, this may mean that the user of the mobile station has to enter another predetermined PIN code with which the mobile station has been configured to start in a predetermined signature mode. Thus, it is possible to use a kind of local authentication.

The invention also concerns a system for digitally signing an electronic form in a secure manner using a mobile station. The system preferably comprises a payment machine and, connected to it, means

for generating the material to be signed and transferring it into the mobile station, said material being as defined above. In this context, `payment machine' may refer to any local or locally operated automated machine capable of communicating over a telecommunication network with a service provider, such as a bank, shop or equivalent.

The payment machine may also be implemented locally in a computer which communicates with the service provider e.g. over the Internet, the service provider providing products and services via the Internet. In this case, the material to be signed is transferred for signature from the computer into the mobile station using a local connection or directly from the service provider's own server without using a local computer and local connection.

According to the invention, the payment machine comprises means for computing a first hash code from the material to be signed. Moreover, the mobile station comprises signing means for the signing of the material transferred into it. The signing means may comprise a memory in which the algorithms and keys required for the signature and encryption are stored, and a processor which is connected to the memory and which processes the material, implementing the signature and possibly encryption. In addition, the payment machine comprises means for verifying the authenticity of the signed material transferred by comparing a hash code signed in the mobile station with a hash code computed from the material before signature.

The system may also comprise a sever which is connected to the payment machine and/or to the mobile station and which is controlled by a second party, such as a bank or credit card company. Such a server may thus be maintained e.g. by a bank and it can be used in the implementation of bank transactions. The server may also comprise means for the verification of

the authenticity of a digital signature made by a mobile station and encrypting and decrypting means for the encryption and/or decryption of material transferred between the server and the payment machine and/or mobile station.

The server may also comprise means for stamping the material with a time stamp and means for filing the transaction of signature of the material after the signature has been authenticated. These can be implemented in a manner known in itself to the skilled person, so they will not be described here in detail.

As compared with prior art, the present invention provides the advantage of facilitating the implementation of payment applications, verification transactions and the like. Thanks to the invention, a mobile station can be reliably used for making a digital signature, and a digital signature can be incorporated in many different applications.

LIST OF ILLUSTRATIONS

In the following, the invention will be described by the aid of a few examples of its preferred embodiments with reference to the attached drawing, wherein

Fig. 1 presents a preferred system according to the present invention;

Fig. 2 presents another preferred system according to the present invention;

Fig. 3 presents a preferred embodiment of the present invention in the form of a flow diagram; and

Fig. 4 is a diagrammatic representation of a preferred example of the generation of the material to be signed in conjunction with the present invention.

The system presented in Fig. 1 comprises a local payment machine (LPM) 2 and, connected to it, means for generating the material to be signed, comprising a form, its identifier, shared data and/or es-

sential information associated with it. In addition, means 4 connected to it for transferring the material to a mobile station. Correspondingly, the mobile station comprises means 1 used by the mobile station (MS) to communicate with the payment machine. In an embodiment, means 1 and 4 are implemented using the Bluetooth technology. A more detailed description of the Bluetooth technology will be found e.g. on WWW page www.bluetooth.com. Other known link access protocols, such as the infrared interface, may also be used.

The system presented in Fig. 1 further comprises a server 8 which is connected via a TCP/IP link to the payment machine 2 and which in this example is managed by a bank. The server further comprises means 9 for verifying the authenticity of the signature - in practice, these means are used to decrypt the encrypted messages received and to compare the digital signatures contained in them with the user information received. Moreover, the server comprises means 11 and 12 for stamping the signed material with a time stamp and filing the signing transaction after the signature has be authenticated. Corresponding verification means may also be comprised in the payment machine, and in this example they are indicated by the number 7. Means 7, 11 and 12 may also have a feature for fetching the required public keys from universal key management servers e.g. via a TCP/IP network.

In the example presented in Fig. 1, the encrypted material, comprising an invoice form and a hash code H1 computed from it, is transferred from the payment machine 2 into the mobile station MS, step 1. In the mobile station, the material, i.e. the invoice form and the payee, payer, amount and reference number of the payment, are presented on the display (10) of the mobile telephone, allowing the user of the mobile station to check what he/she is signing. Using the mobile station MS, the user then signs the material and

the hash code H1 computed from it. The material with the digitally signed hash code $H1_{ds}$ added to it is transferred into the payment machine 2, step 2. The messages transmitted between the payment machine 2 the mobile station MS can be encrypted using public and private keys of the mobile station user and the payment machine. After the authenticity of the signature has been verified in the payment machine 2, a clearing message is sent from the payment machine to the bank, step 3. Clearing is a known practice generally used in banking, so it will not be described here in detail.

Reference is now made to Fig. 2, which presents a system corresponding to Fig. 1, but in this case the system is used in a somewhat different manner. First, the material generated in the payment machine, e.g. a form, is transferred to the bank, step 1. Next, in the payment machine, a hash code H1 is computed from the material and transferred to the mobile station for signature, step 2. The transfer can be implemented using a local link, e.g. a Bluetooth connection. In the mobile station, the message received is signed digitally, whereupon the signed and possibly encrypted material is sent to the bank, step 3. In the bank, the hash code H1 computed from the material received from the payment machine is compared with the digitally signed hash code $H1_{ds}$ received from the mobile station, and if the two hash codes match, then the signing transaction is approved. After this, using a server, a time stamp is added and the signing transaction thus obtained is filed. The bank may also be some other corresponding service provider, such as a credit card company, in which case, in addition to the above description, a confirmation of authenticity of the signature is sent to the bank, payment machine or other service provider. In this case, the credit card company, after confirming the signature, takes responsibility for the transaction.

Referring to Fig. 3, a preferred embodiment of the invention will be described. First, the material to be signed by means of a mobile station is generated, block 31. From the material, a first hash code H1 is computed, block 32. Next, block 45, a check is performed to establish whether the material has to be encrypted before transmission. If the material has to be encrypted, then the procedure goes on to block 46 and the material is encrypted using the mobile station user's public key. After the encryption, the procedure goes on to block 33. If the material need not be encrypted, then action proceeds directly to block 33, where the material is transferred to the mobile station. Next, the procedure goes on to block 34, and the user checks the material or the essential information in it, presented on the display of the mobile station, in other words, the user checks whether e.g. the payee and the payment in an invoice are correct. If the payer agrees, in block 35, then action proceeds to block 37 and the material is signed. If the payer does not agree in block 35, then the procedure goes on to block 36, where a reject message is sent to the sender of the material, e.g. a payment machine, and the process is stopped. From block 37, action proceeds to block 38, where a data aggregate is generated from the digital signature and hash code and possibly from the material received, comprising e.g. the essential information contained in the form, block 38. After that, the data aggregate is transferred to the payment machine, block 39, from where the process goes on to block 40, where the hash code computed from the transferred material is compared with the signed hash code. If the hash codes match, block 41, then the signature is accepted and the further actions defined are carried out.

If in block 40 the hash codes did not match, then the procedure can be repeated. At this point it

is possible to use a counter to check that the material will not be sent more times than previously agreed. From block 40, the procedure goes on to block 43, where the value of a counter k = k + 1 is incremented by one, whereupon action proceeds to block 44, where the value of the counter is checked, this value indicating the number of times the material has been transferred to the mobile station. If the value exceeds a pre-agreed limit, then the procedure goes on to block 42 and a reject message is sent to the mobile station. If the value of the counter is smaller than the pre-agreed limit, then the procedure returns to block 31 and the process is repeated.

Fig. 4 illustrates a preferred way of digitally generating and signing the form or material. The material to be transferred to the mobile station comprises a form identifier, block 51, all the forms used having unique identifiers. Associated with the form identifier is a form template, block 52; based on these, the applications, the client and the provider of the application know exactly what type of form is being used in each case. When the material is being generated, the form identifier and the form template are chained sequentially as illustrated in Fig. 4, whereupon a first hash code is computed from them, block 54.

In many cases, form data is added to the form, block 53, even before the form is transferred to the mobile station for signature. In this case, the form identifier and the form data are concatenated in the order indicated in Fig. 4 and the bit sequence obtained from them is further concatenated with sixteen random bytes, block 55. The first hash code from block 54 is combined with these data.

At this point, the material is ready to be transferred to the mobile station, whereupon a second hash code is computed from it, block 56. In practice,

the second hash code is computed in the mobile station and added to the message to be signed, block 57. Likewise, user data, which the mobile station user may have complemented with personal information as needed, has been added to the message to be signed. To this message to be signed are preferably also added the 16 random bytes from block 55, thus making it possible to verify the authenticity of the signed message generated by the party transferring the material and the mobile station user. After the random bytes, the user data and the second hash code have been set in sequence, the message is signed digitally in the user's mobile station. After this, the message can be transmitted further to a second party, to a payment machine or other original source of the material.

In summary, let it be further stated that the invention purports to implement a method and system in which a user, a service provider and a bank, which are mentioned as an example, are able to verify the authenticity of a digital signature. The objective is to enable the material to be signed to be bound to some user data, format and a digital signature made by the user. In other words, it must be possible to bind the signature to a certain kind of chain, which in practice corresponds to the currently used chain in which the user confirms a purchase by his/her own manual signature. Similarly, the object of the method is to identify the signatory in a reliable manner as required and intended by the legislator.

The invention is not restricted to the examples described above, but many variations are possible within the limits of the sphere of protection defined by the claims.

CLAIMS

1. Method for digitally signing an electronic form in a secure manner by means of a mobile station, said method comprising the steps of

transferring the material to be signed, which comprises the form, its identifier, shared information, and/or essential information added to it, to the mobile station, characterized in that

a first hash code (H1) is computed from the material to be signed;

the hash code is added to the material, to be transferred to the mobile station;

the material transferred to the mobile station is signed digitally by means of the mobile station; and

the authenticity of the signed and transferred material is verified by comparing the signed hash code with the hash code computed from the material before signature.

2. Method as defined in claim 1, characterized in that

the material transferred to the mobile station for signature is transferred to a second party; and

the signed material is transferred to the second party, whereupon the second party verifies the authenticity of the signature.

3. Method as defined in claim 1 or 2, characterized in that

the material is encrypted before being transferred between the mobile station and the second party; and

the encrypted material is decrypted before any treatment of the material, such as signature and verification of authenticity.

4. Method as defined in any one of the preceding claims 1 - 3, characterized in that

the form is generated using a pre-agreed form template provided with an identifier, the essential information being filled in in the form template before it is transferred to the mobile station.

5. Method as defined in any one of the preceding claims 1 - 4, characterized in that

the hash code is generated using a hash function.

6. Method as defined in any one of the preceding claims 1 - 5, characterized in that

the signature and/or encryption of the message is implemented using a public and private key method.

7. Method as defined in any one of the preceding claims 1 - 6, characterized in that

the material and/or part of it is presented in the mobile station before the material is signed.

8. Method as defined in any one of the preceding claims 1 - 7, characterized in that

the mobile station is started in signature mode before the transfer of the material into the mobile station.

9. Method as defined in any one of the preceding claims 1 - 8, characterized in that

the material is stamped with a time stamp; and

the transaction of signature of the material is filed after the signature has been authenticated.

10. System for digitally signing an electronic form in a secure manner by means of a mobile station (MS), said system comprising

a payment machine (2);

means (3) connected to the payment machine for the generation of the material to be signed, said material comprising a form, its identifier, shared data, and/or essential information added to it; and

means (4) connected to the payment machine for the transfer of the material into the mobile station (MS), c h a r a c t e r i z e d in that

the payment machine comprises means (5) for computing a first hash code (H1) from the material to be signed;

the mobile station comprises signing means (6) for the signing of the material transferred into it; and

the payment machine comprises means (7) for verifying the authenticity of the signed and transferred material by comparing s signed hash code ($H1_{ds}$) with the hash code (H1) computed from the material before signature.

11. System as defined in claim 10, c h a r a c t e r i z e d in that the system comprises

a server (8) connected to the payment machine (2) and the mobile station (MS) and controlled by a third party; and

the mobile station comprises means for encrypting the signed material.

12. System as defined in claim 10 or 11, c h a r a c t e r i z e d in that the server (8) comprises

means (9) for the verification of authenticity of the digital signature.

13. System as defined in any one of the preceding claims 10 - 12, c h a r a c t e r i z e d in that the mobile station comprises

means (10) for presenting the material and/or part of it in the mobile station before the signing of the material.

14. System as defined in any one of the preceding claims 10 - 13, c h a r a c t e r i z e d in that the server (8) comprises

means (11) for stamping the material with a time stamp; and

means (12) for filing the transaction of signing of the material after the signature has been authenticated.

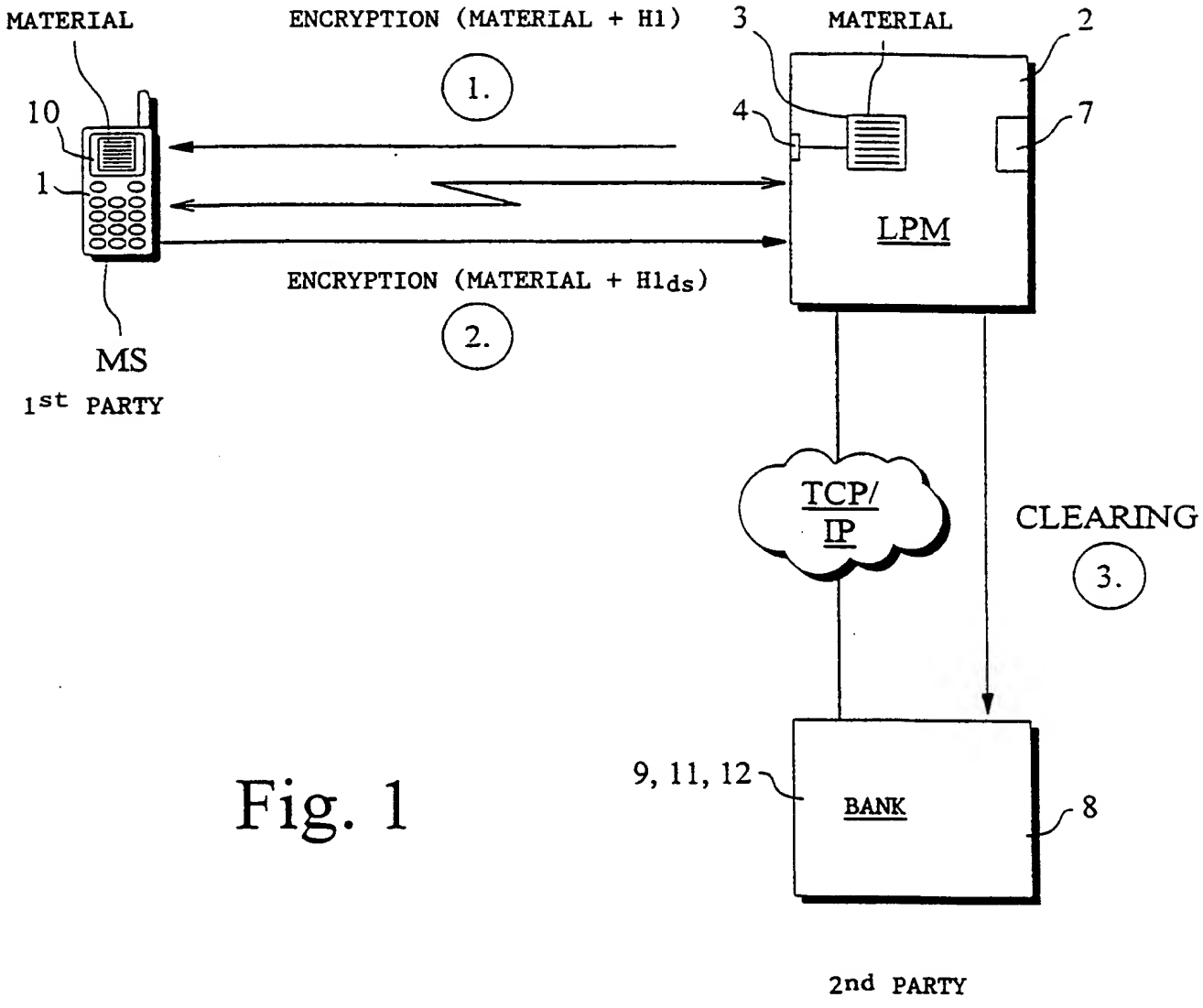

MATERIAL
ENCRYPTION (MATERIAL + H1)
3
MATERIAL
2
1.
10
4
7
1
LPM
ENCRYPTION (MATERIAL + H1ds)
2.
MS
1st PARTY
TCP/
IP
CLEARING
3.
9, 11, 12
BANK
8
2nd PARTY

Fig. 1

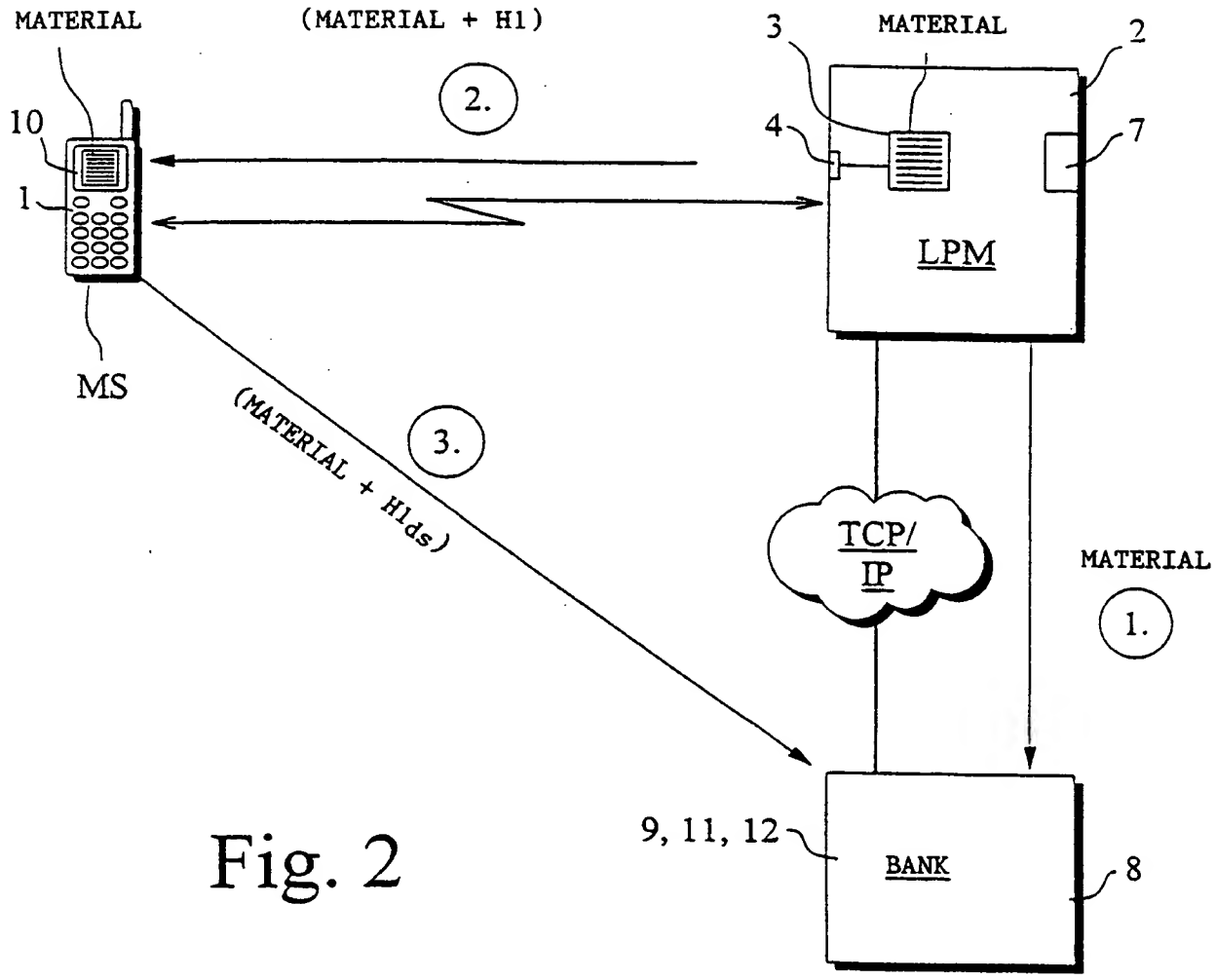

MATERIAL
(MATERIAL + H1)
2.
3
MATERIAL
2
10
4
7
1
LPM
MS
(MATERIAL + H1ds)
3.
TCP/
IP
MATERIAL
1.
9, 11, 12
BANK
8

Fig. 2

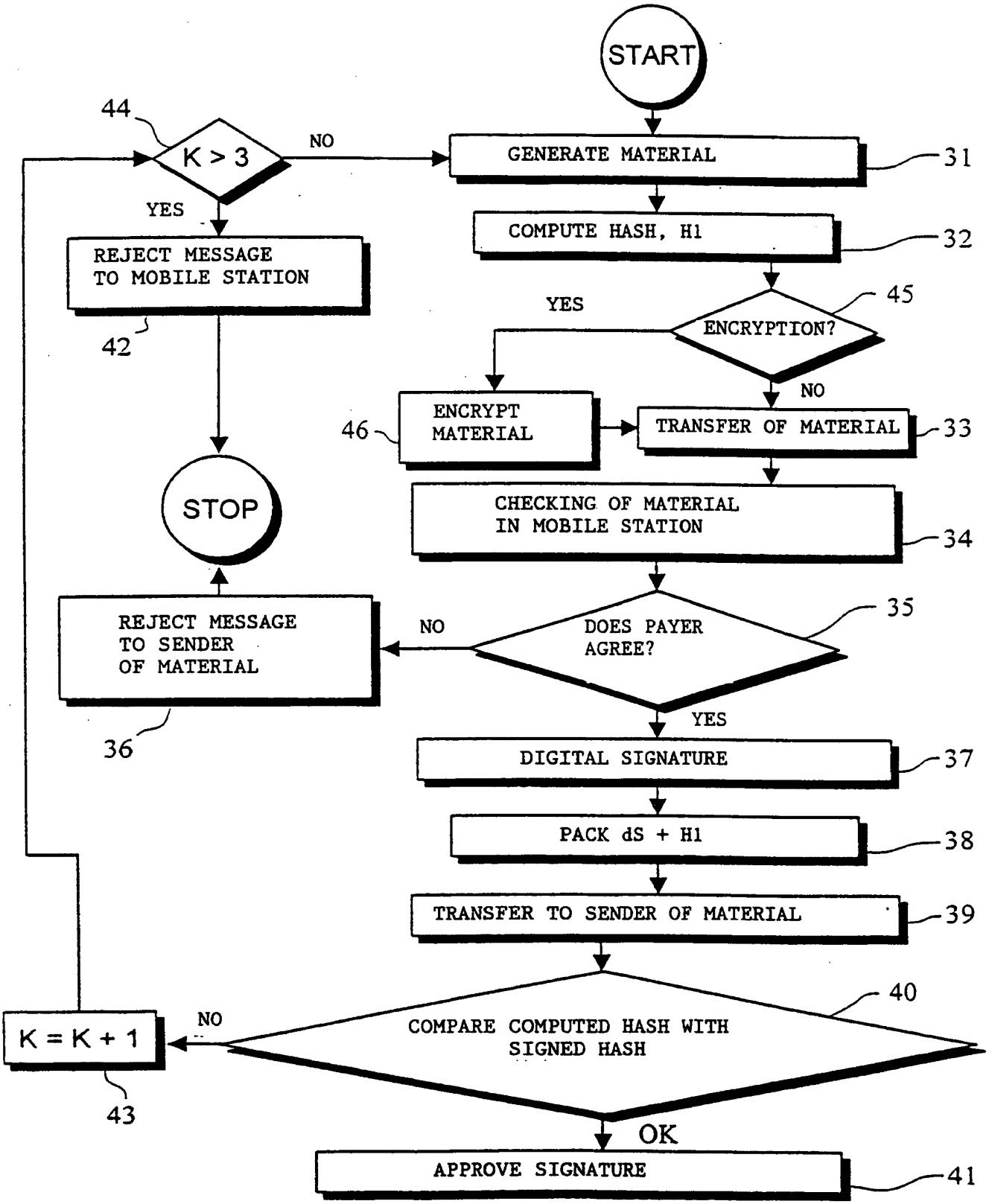

START
GENERATE MATERIAL
31
COMPUTE HASH, H1
32
ENCRYPTION?
45
YES
NO
ENCRYPT MATERIAL
46
TRANSFER OF MATERIAL
33
CHECKING OF MATERIAL IN MOBILE STATION
34
DOES PAYER AGREE?
35
NO
YES
REJECT MESSAGE TO SENDER OF MATERIAL
36
DIGITAL SIGNATURE
37
PACK dS + H1
38
TRANSFER TO SENDER OF MATERIAL
39
COMPARE COMPUTED HASH WITH SIGNED HASH
40
NO
OK
APPROVE SIGNATURE
41
K = K + 1
43
K > 3
44
NO
YES
REJECT MESSAGE TO MOBILE STATION
42
STOP

Fig. 3

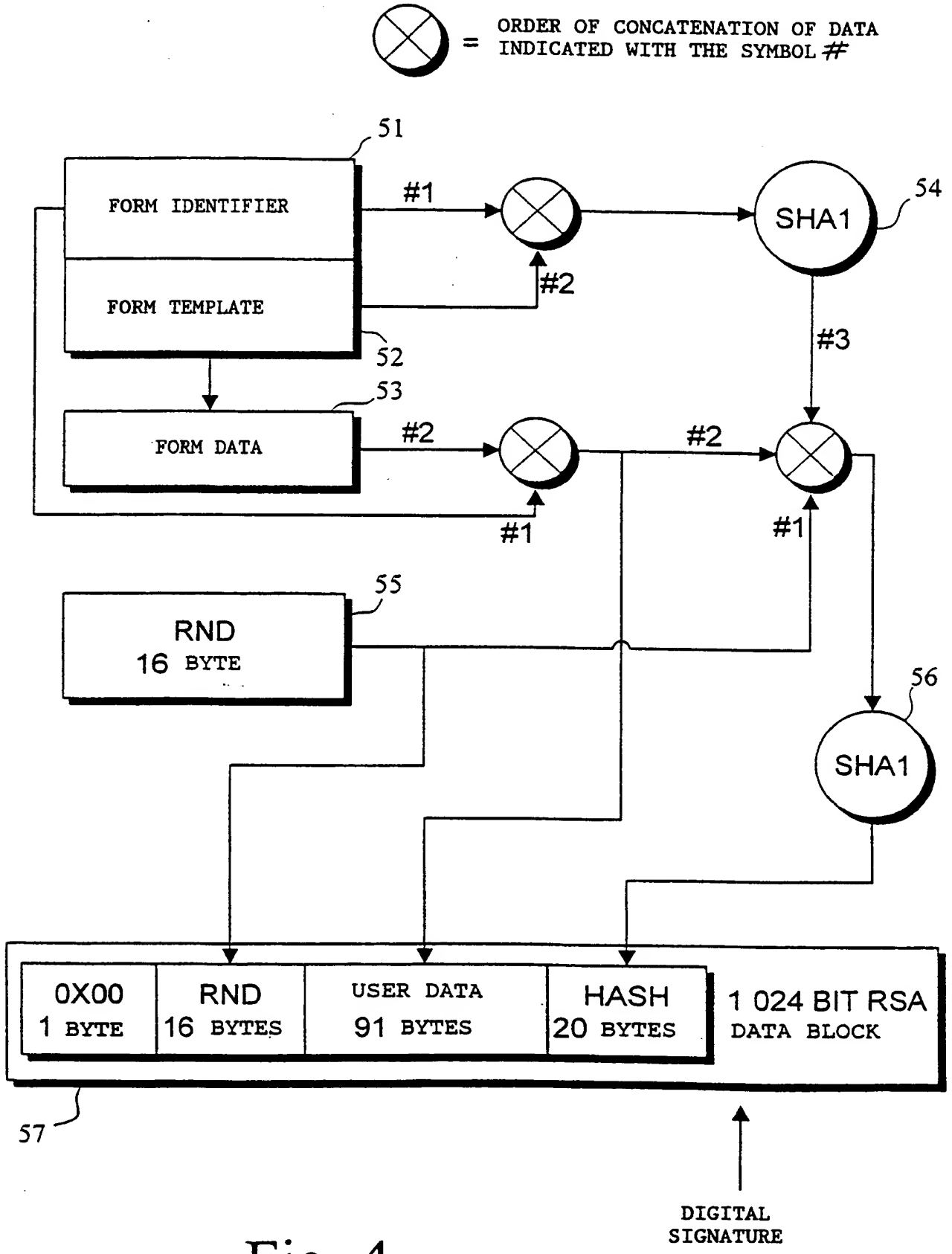

= ORDER OF CONCATENATION OF DATA INDICATED WITH THE SYMBOL #
51
FORM IDENTIFIER
FORM TEMPLATE
52
#1
#2
SHA1
54
#3
53
FORM DATA
#2
#2
#1
#1
55
RND
16 BYTE
56
SHA1
0X00
1 BYTE
RND
16 BYTES
USER DATA
91 BYTES
HASH
20 BYTES
1 024 BIT RSA
DATA BLOCK
57
DIGITAL
SIGNATURE

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 99/01036

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0689316 A2 (AT & T CORP.), 27 December 1995 (27.12.95), figure 1, abstract --	1-14
X	William Stallings, "Data and Computer Communications", 1997, Prentice-Hall International, Inc., (London), page 638 - page 649, figure 18.11(b) --	1
X	US 5018196 A (K. TAKARAGI ET AL.), 21 May 1991 (21.05.91), figure 1, abstract --	1-14
A	WO 9411849 A1 (VATANEN, HARRI, TAPANI), 26 May 1994 (26.05.94), cited in the application --	1-14

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 April 2000	18 -04- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/AE Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 99/01036

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5221838 A (JOSE GUTMAN ET AL.), 22 June 1993 (22.06.93), cited in the application -- --------	1-14

INTERNATIONAL SEARCH REPORT

Information on patent family members

02/12/99

International application No.
PCT/FI 99/01036

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0689316 A2	27/12/95	CA 2149067 A	23/12/95
		JP 8032575 A	02/02/96
US 5018196 A	21/05/91	JP 2112794 C	21/11/96
		JP 8027812 B	21/03/96
		JP 62254543 A	06/11/87
		US 4885777 A	05/12/89
		DE 3687934 A	15/04/93
		EP 0214609 A,B	18/03/87
		JP 62056043 A	11/03/87
		JP 2170184 A	29/06/90
WO 9411849 A1	26/05/94	AT 159602 T	15/11/97
		DE 69314804 D,T	12/02/98
		EP 0669031 A,B	30/08/95
		SE 0669031 T3	
		ES 2107689 T	01/12/97
		FI 925135 A	12/05/94
		FI 934995 A	12/05/94
		GR 3025393 T	27/02/98
		NO 951814 A	09/05/95
US 5221838 A	22/06/93	CA 2096730 A,C	25/06/92
		EP 0564469 A	13/10/93
		SE 0564469 T3	
		EP 0940760 A	08/09/99
		JP 6501329 T	10/02/94
		KR 9707003 B	01/05/97
		WO 9211598 A	09/07/92

By Express Mail
No. EL489599

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 99/01036

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0689316 A2 (AT & T CORP.), 27 December 1995 (27.12.95), figure 1, abstract --	1-14
X	William Stallings, "Data and Computer Communications", 1997, Prentice-Hall International, Inc., (London), page 638 - page 649, figure 18.11(b) --	1
X	US 5018196 A (K. TAKARAGI ET AL.), 21 May 1991 (21.05.91), figure 1, abstract --	1-14
A	WO 9411849 A1 (VATANEN, HARRI, TAPANI), 26 May 1994 (26.05.94), cited in the application --	1-14

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 April 2000	18 -04- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/AE Telephone No. +46 8 782 25 00

By Express Mail
No. EL489599408US

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 99/01036

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5221838 A (JOSE GUTMAN ET AL.), 22 June 1993 (22.06.93), cited in the application	1-14

By Express Mail
No. EL489599[redacted]

INTERNATIONAL SEARCH REPORT

Information on patent family members

02/12/99

International application No.
PCT/FI 99/01036

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0689316 A2	27/12/95	CA 2149067 A	23/12/95
		JP 8032575 A	02/02/96
US 5018196 A	21/05/91	JP 2112794 C	21/11/96
		JP 8027812 B	21/03/96
		JP 62254543 A	06/11/87
		US 4885777 A	05/12/89
		DE 3687934 A	15/04/93
		EP 0214609 A,B	18/03/87
		JP 62056043 A	11/03/87
		JP 2170184 A	29/06/90
WO 9411849 A1	26/05/94	AT 159602 T	15/11/97
		DE 69314804 D,T	12/02/98
		EP 0669031 A,B	30/08/95
		SE 0669031 T3	
		ES 2107689 T	01/12/97
		FI 925135 A	12/05/94
		FI 934995 A	12/05/94
		GR 3025393 T	27/02/98
		NO 951814 A	09/05/95
US 5221838 A	22/06/93	CA 2096730 A,C	25/06/92
		EP 0564469 A	13/10/93
		SE 0564469 T3	
		EP 0940760 A	08/09/99
		JP 6501329 T	10/02/94
		KR 9707003 B	01/05/97
		WO 9211598 A	09/07/92

By Express Mail
No. EL489599408US

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No
PCT/FI99/01036

I. Basis of the report

1. With regard to the elements of the international application *

- ☐ the international application as originally filed
- ☒ the description:
  - pages 1-13, as originally filed
  - pages _____, filed with the demand
  - pages _____, filed with the letter of _____
- ☒ the claims:
  - pages _____, as originally filed
  - pages _____, as amended (together with any statement) under article 19
  - pages _____, filed with the demand
  - pages 14-17, filed with the letter of 24.01.2001
- ☒ the drawings:
  - pages 1-4, as originally filed
  - pages _____, filed with the demand
  - pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description
  - pages _____, as originally filed
  - pages _____, filed with the demand
  - pages _____, filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language English which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b))
- ☒ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form
- ☐ filed together with the international application in computer readable form
- ☐ furnished subsequently to this Authority in written form
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

4 ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos _____
- ☐ the drawings, sheet/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2 (c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

By Express Mail
No. EL489599408US

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FI00/01036

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Statement

Novelty (N)	Claims	1-14	YES
	Claims		NO
Inventive step (IS)	Claims	1-14	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-14	YES
	Claims		NO

2 Citations and explanations (Rule 70.7)

D1: EP 689316 A2
D2: US 5018196 A

The invention relates to a method and a system for digitally signing an electronic form in a secure manner by means of a mobile station. The most significant feature is that a hash code is used for verifying the authenticity of the signed and transferred material. Hash code in the signed material is compared with hash code computed from the material before signing.

In amended claims 1 and 10 the differences between the invention and the state-of-the-art technology as represented by D1 and D2 are clearly defined.

Therefore, the requirements of novelty and inventive step are now considered fulfilled.

Also the requirement of industrial applicability is fulfilled.

By Express Mail
No. EL489599408US

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 12714S	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FI99/01036	International filing date *(day month year)* 15.12.1999	Priority date *(day month year)* 16.12.1998
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant Sonera Smarttrust OY et al		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 4 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand 05.07.2000	Date of completion of this report 20.03.2001
Name and mailing address of the IPEA/SE Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Telex 17978 PATOF S Facsimile No 08-667 72 88	Authorized officer Rune Bengtsson /OGU Telephone No 08-782 25 00

Form PCT/IPEA/409 (cover sheet) (January 1998)

By Express Mail
No. EL489599408US

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

CLAIMS

1. Method for digitally signing an electronic form in a secure manner by means of a mobile station, said method comprising the steps of

transferring the material to be signed, which comprises the form, its identifier, shared information, and/or essential information added to it, to the mobile station, characterized in that

a first hash code (H1) is computed from the material to be signed;

the hash code is added to the material, to be transferred to the mobile station;

the material transferred to the mobile station is signed digitally by means of the mobile station; and

the authenticity of the signed and transferred material is verified by comparing the signed hash code with the hash code computed from the material before signature.

2. Method as defined in claim 1, characterized in that

the material transferred to the mobile station for signature is transferred to a second party; and

the signed material is transferred to the second party, whereupon the second party verifies the authenticity of the signature.

3. Method as defined in claim 1 or 2, characterized in that

the material is encrypted before being transferred between the mobile station and the second party; and

the encrypted material is decrypted before any treatment of the material, such as signature and verification of authenticity.

4. Method as defined in any one of the preceding claims 1 - 3, characterized in that

the form is generated using a pre-agreed form template provided with an identifier, the essential information being filled in in the form template before it is transferred to the mobile station.

5. Method as defined in any one of the preceding claims 1 - 4, characterized in that

the hash code is generated using a hash function.

6. Method as defined in any one of the preceding claims 1 - 5, characterized in that

the signature and/or encryption of the message is implemented using a public and private key method.

7. Method as defined in any one of the preceding claims 1 - 6, characterized in that

the material and/or part of it is presented in the mobile station before the material is signed.

8. Method as defined in any one of the preceding claims 1 - 7, characterized in that

the mobile station is started in signature mode before the transfer of the material into the mobile station.

9. Method as defined in any one of the preceding claims 1 - 8, characterized in that

the material is stamped with a time stamp; and

the transaction of signature of the material is filed after the signature has been authenticated.

10. System for digitally signing an electronic form in a secure manner by means of a mobile station (MS), said system comprising

a payment machine (2);

means (3) connected to the payment machine for the generation of the material to be signed, said material comprising a form, its identifier, shared data, and/or essential information added to it; and

means (4) connected to the payment machine for the transfer of the material into the mobile station (MS), characterized in that

the payment machine comprises means (5) for computing a first hash code (H1) from the material to be signed;

the mobile station comprises signing means (6) for the signing of the material transferred into it; and

the payment machine comprises means (7) for verifying the authenticity of the signed and transferred material by comparing s signed hash code ($H1_{as}$) with the hash code (H1) computed from the material before signature.

11. System as defined in claim 10, characterized in that the system comprises

a server (8) connected to the payment machine (2) and the mobile station (MS) and controlled by a third party; and

the mobile station comprises means for encrypting the signed material.

12. System as defined in claim 10 or 11, characterized in that the server (8) comprises

means (9) for the verification of authenticity of the digital signature.

13. System as defined in any one of the preceding claims 10 - 12, characterized in that the mobile station comprises

means (10) for presenting the material and/or part of it in the mobile station before the signing of the material.

14. System as defined in any one of the preceding claims 10 - 13, characterized in that the server (8) comprises

means (11) for stamping the material with a time stamp; and

Express Mail
No. EL489599408US

WO 00/39958 PCT/FI99/01036

means ~~(12)~~ for filing ~~the~~ transaction of signing of the ~~material after~~ the signature has been ~~authenticated~~.

RECORD COPY

PCT REQUEST

12714S

Original (for **SUBMISSION**) - printed on 14.12.1999 02:11:01 PM

0	**For receiving Office use only**	
0-1	International Application No.	PCT/FI 9 9 / 0 1 0 3 6
0-2	International Filing Date	1 5 DEC 1999 (15. 12. 99)
0-3	Name of receiving Office and "PCT International Application"	The Finnish Patent Office PCT International Application
0-4	**Form - PCT/RO/101 PCT Request**	
0-4-1	Prepared using	**PCT-EASY Version 2.90 (updated 15.10.1999)**
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	**National Board of Patents and Registration (Finland) (RO/FI)**
0-7	**Applicant's or agent's file reference**	**12714S**
I	**Title of invention**	**METHOD AND SYSTEM FOR IMPLEMENTING A DIGITAL SIGNATURE**
II	**Applicant**	
II-1	This person is:	**applicant only**
II-2	Applicant for	**all designated States except US**
II-4	Name	**SONERA OYJ**
II-5	Address:	**Teollisuuskatu 15 FIN-00510 Helsinki Finland**
II-6	State of nationality	**FI**
II-7	State of residence	**FI**
III-1	**Applicant and/or inventor**	
III-1-1	This person is:	**applicant and inventor**
III-1-2	Applicant for	**US only**
III-1-4	Name (LAST, First)	**VATANEN, Harri**
III-1-5	Address:	**40 Alma Road Windsor, Berkshire SL4 3HJ United Kingdom**
III-1-6	State of nationality	**FI**
III-1-7	State of residence	**GB**

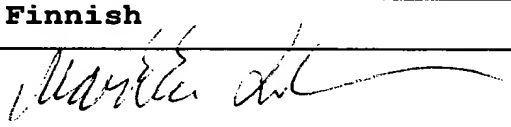
PCT REQUEST 12714S

Original (for **SUBMISSION**) - printed on 14.12.1999 02:11:01 PM

IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name	PAPULA REIN LAHTELA OY
IV-1-2	Address:	P.O. Box 981 (Fredrikinkatu 61 A) FIN-00101 Helsinki Finland
IV-1-3	Telephone No.	+358 9 3480 060
IV-1-4	Facsimile No.	+358 9 3480 0630
IV-1-5	e-mail	papula@papula.fi
V	**Designation of States**	
V-1	Regional Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AP: GH GM KE LS MW SD SL SZ TZ UG ZW and any other State which is a Contracting State of the Harare Protocol and of the PCT EA: AM AZ BY KG KZ MD RU TJ TM and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE and any other State which is a Contracting State of the European Patent Convention and of the PCT OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG and any other State which is a member State of OAPI and a Contracting State of the PCT
V-2	National Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AE AL AM AT AU AZ BA BB BG BR BY CA CH&LI CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
V-5	**Precautionary Designation Statement** In addition to the designations made under items V-1, V-2 and V-3, the applicant also makes under Rule 4.9(b) all designations which would be permitted under the PCT except any designation(s) of the State(s) indicated under item V-6 below. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit.	
V-6	**Exclusion(s) from precautionary designations**	NONE

PCT REQUEST 12714S

Original (for **SUBMISSION**) - printed on 14.12.1999 02:11:01 PM

VI-1	**Priority claim of earlier national application**		
VI-1-1	Filing date	16 December 1998 (16.12.1998)	
VI-1-2	Number	982728	
VI-1-3	Country	FI	
VII-1	**International Searching Authority Chosen**	Swedish Patent Office (ISA/SE)	
VIII	**Check list**	number of sheets	electronic file(s) attached
VIII-1	Request	3	-
VIII-2	Description	13	-
VIII-3	Claims	3	-
VIII-4	Abstract	1	12714s.txt
VIII-5	Drawings	4	-
VIII-7	TOTAL	24	
	Accompanying items	paper document(s) attached	electronic file(s) attached
VIII-8	Fee calculation sheet	✓	-
VIII-10	Copy of general power of attorney	✓	-
VIII-16	PCT-EASY diskette	-	diskette
VIII-17	Other (specified):	Official action / FI 982728	-
VIII-18	**Figure of the drawings which should accompany the abstract**	1	
VIII-19	**Language of filing of the international application**	Finnish	
IX-1	**Signature of applicant or agent**		
IX-1-1	Name	PAPULA REIN LAHTELA OY	
IX-1-2	Name of signatory	Markku Simmelvuo	

FOR RECEIVING OFFICE USE ONLY

10-1	**Date of actual receipt of the purported international application**	15 DEC 1999 (15 -12- 1999)
10-2	**Drawings:**	
10-2-1	Received	
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	ISA/SE
10-6	**Transmittal of search copy delayed until search fee is paid**	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	**Date of receipt of the record copy by the International Bureau**	26 JANUARY 2000 (26. 01. 00)

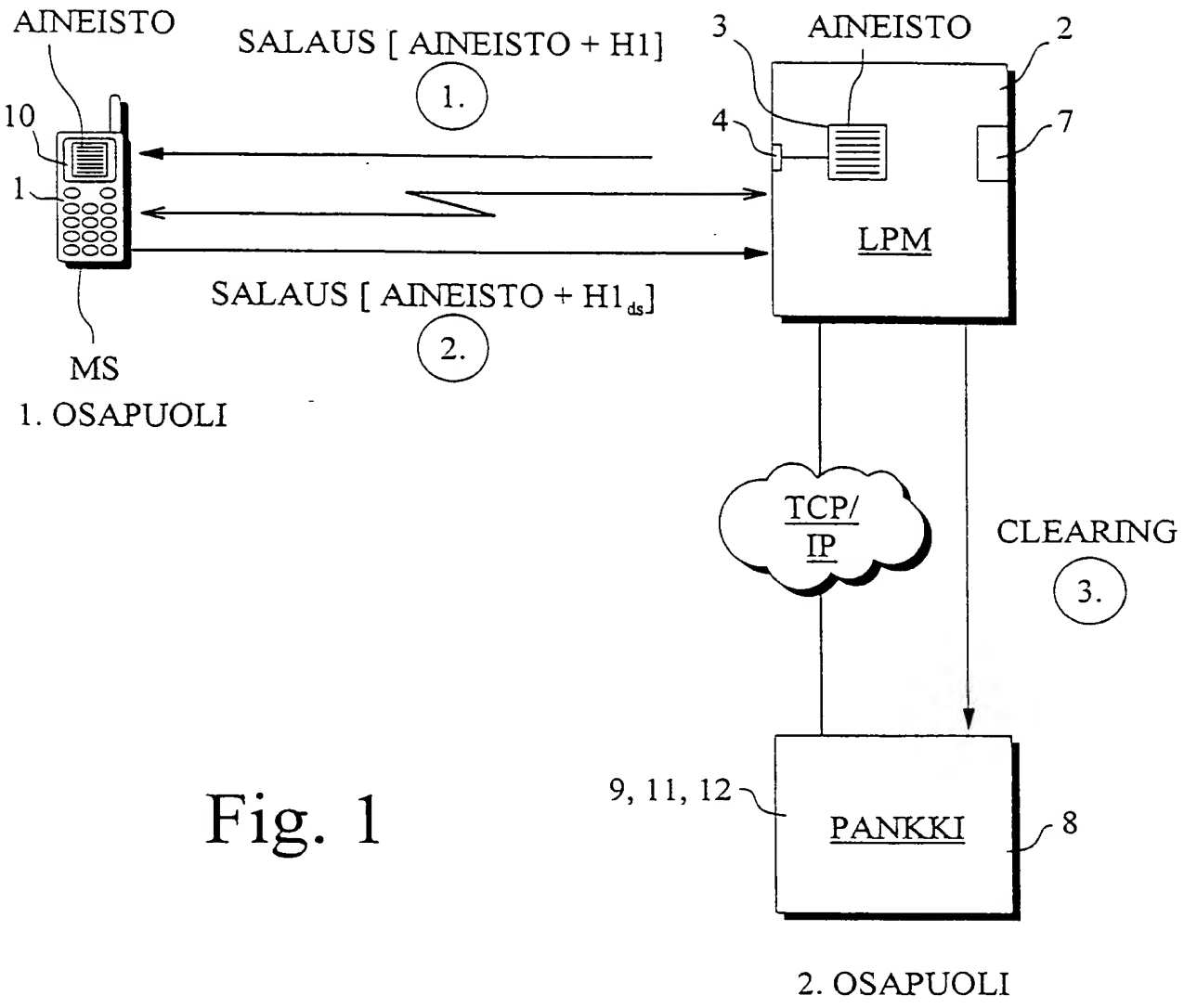

AINEISTO
SALAUS [AINEISTO + H1]
1.
3
AINEISTO
2
10
4
7
1
LPM
SALAUS [AINEISTO + H1ds]
2.
MS
1. OSAPUOLI
TCP/
IP
CLEARING
3.
9, 11, 12
PANKKI
8
2. OSAPUOLI

Fig. 1

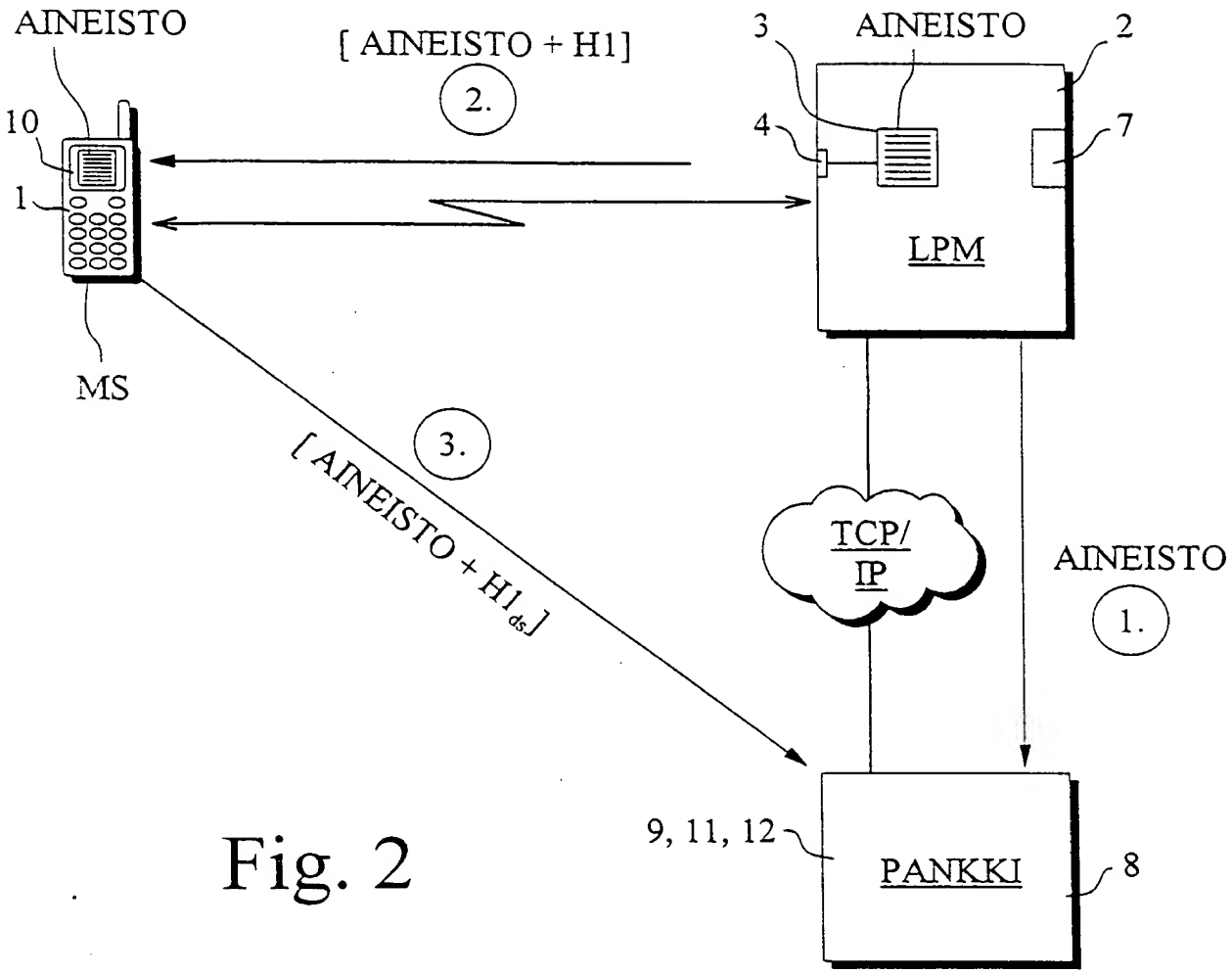

AINEISTO
[AINEISTO + H1]
2.
3
AINEISTO
2
10
4
7
1
LPM
MS
3.
[AINEISTO + H1ds]
TCP/
IP
AINEISTO
1.
9, 11, 12
PANKKI
8

Fig. 2

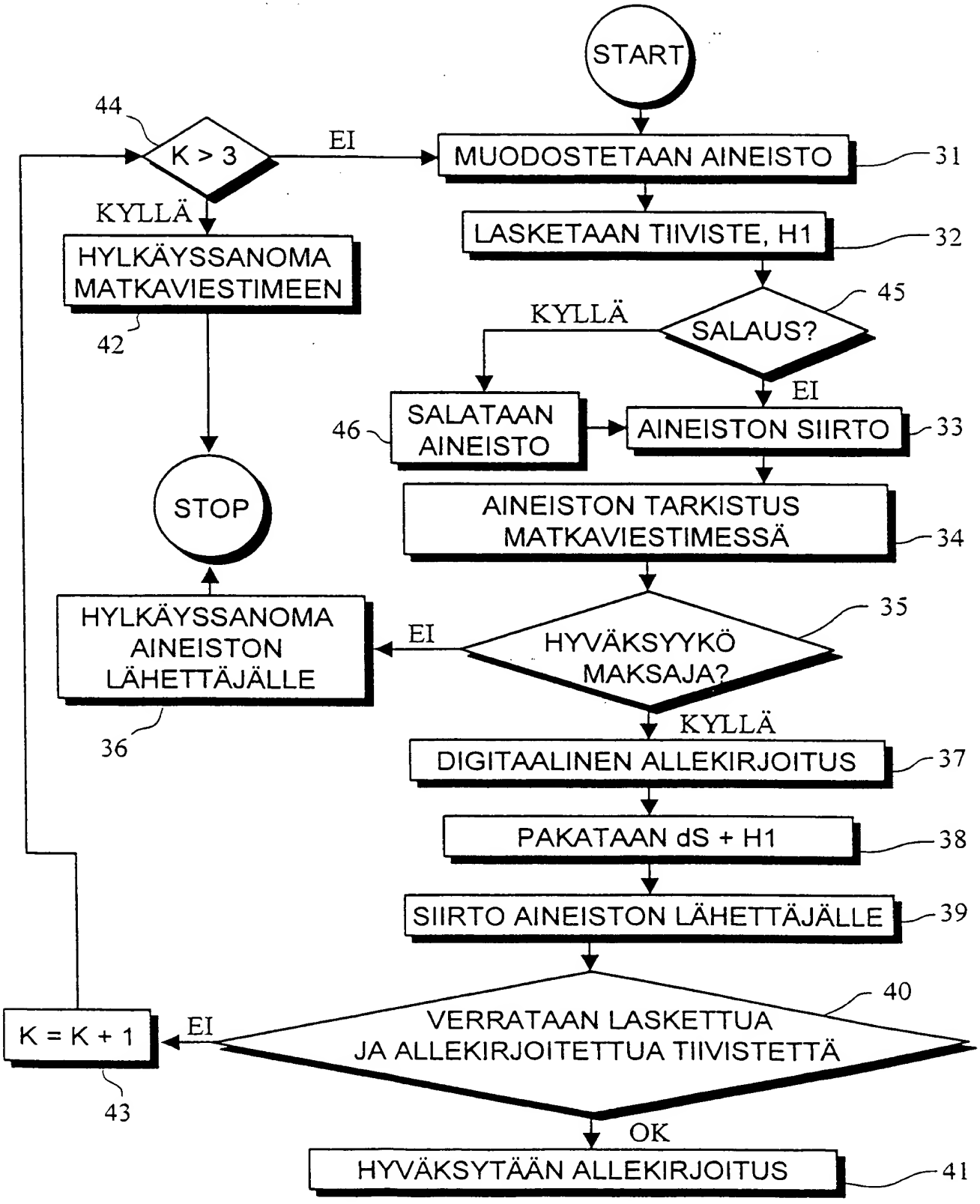

START
MUODOSTETAAN AINEISTO
31
LASKETAAN TIIVISTE, H1
32
SALAUS?
45
KYLLÄ
EI
SALATAAN AINEISTO
46
AINEISTON SIIRTO
33
AINEISTON TARKISTUS MATKAVIESTIMESSÄ
34
HYVÄKSYYKÖ MAKSAJA?
35
EI
KYLLÄ
HYLKÄYSSANOMA AINEISTON LÄHETTÄJÄLLE
36
DIGITAALINEN ALLEKIRJOITUS
37
PAKATAAN dS + H1
38
SIIRTO AINEISTON LÄHETTÄJÄLLE
39
VERRATAAN LASKETTUA JA ALLEKIRJOITETTUA TIIVISTETTÄ
40
EI
OK
K = K + 1
43
HYVÄKSYTÄÄN ALLEKIRJOITUS
41
K > 3
44
EI
KYLLÄ
HYLKÄYSSANOMA MATKAVIESTIMEEN
42
STOP

Fig. 3

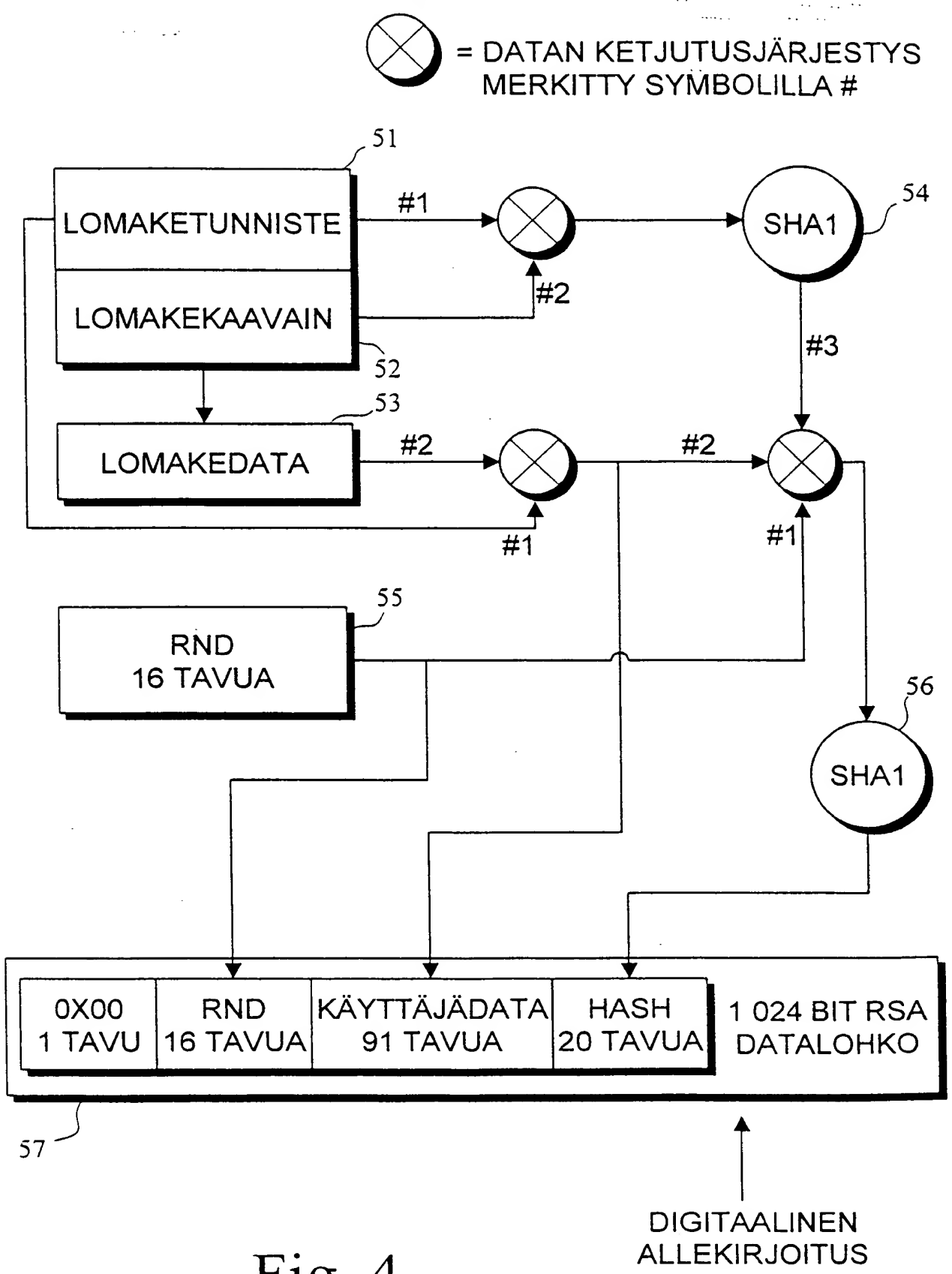

= DATAN KETJUTUSJÄRJESTYS
MERKITTY SYMBOLILLA #
51
LOMAKETUNNISTE
LOMAKEKAAVAIN
52
#1
#2
SHA1
54
#3
53
LOMAKEDATA
#2
#2
#1
#1
55
RND
16 TAVUA
56
SHA1
0X00
1 TAVU
RND
16 TAVUA
KÄYTTÄJÄDATA
91 TAVUA
HASH
20 TAVUA
1 024 BIT RSA
DATALOHKO
57
DIGITAALINEN
ALLEKIRJOITUS

Fig. 4

MENETELMÄ JA JÄRJESTELMÄ DIGITAALISEN ALLEKIRJOITUKSEN TOTEUTTAMISEKSI

Esillä oleva keksintö liittyy tietoliikennejärjestelmiin ja digitaalisen tiedon allekirjoitus- ja salaustekniikkaan. Erityisesti keksintö liittyy uudentyyppiseen ja kehittyneeseen menetelmään ja järjestelmään, jonka avulla lomake tai muu allekirjoitettava sähköisessä muodossa oleva tieto voidaan allekirjoittaa ja varmistua allekirjoituksen ja allekirjoittajan oikeellisuudesta.

TEKNIIKAN TASO

Entuudestaan on tunnettua käyttää digitaalista matkaviestintä, kuten GSM-järjestelmän (Global System for Mobile Communications, GSM) matkaviestintä, kaupallisiin transaktioihin, kuten laskun tai maksun maksamiseen sähköisesti. Patenttijulkaisusta US 5,221,838 tunnetaan laite, jota voidaan käyttää maksamiseen. Julkaisussa on kuvattu sähköinen maksujärjestelmä, jossa maksupäätteenä käytetään langattomaan ja/tai langalliseen tiedonsiirtoon kykenevää päätelaitetta. Julkaisun mukaiseen päätelaitteeseen kuuluu kortinlukija, näppäimistö, ja viivakoodin lukija tietojen syöttämiseksi ja näyttö maksuinformaation esittämiseksi.

Patenttijulkaisusta WO 94/11849 tunnetaan menetelmä tietoliikennepalveluiden käyttämiseksi ja maksuliikenteen suorittamiseksi matkapuhelinjärjestelmällä. Julkaisussa kuvataan järjestelmä, johon kuuluu päätelaite, joka on yhteydessä televerkon kautta palveluntarjoajan keskustietokoneeseen, joka sisältää palveluntarjoajan maksujärjestelmän. Matkapuhelinverkon päätelaitteeseen eli matkaviestimeen voidaan lisätä tilaajan tunnistusyksikkö, joka käsittää tilaajatiedot tilaajan tunnistamiseksi ja teleliikenteen salaamiseksi. Tiedot voidaan lukea päätelaitteeseen käy-

tettäväksi matkaviestimissä. Esimerkkinä julkaisussa mainitaan GSM-järjestelmä, jossa käytetään SIM-korttia (Subscriber Identity Module, SIM) tilaajan tunnistusyksikkönä.

Julkaisun WO 94/11849 mukaisessa järjestelmässä matkaviestin on yhteydessä matkapuhelinverkon tukiasemaan. Julkaisun mukaan yhteys muodostetaan edelleen maksujärjestelmään ja maksettava määrä samaten kuin tilaajan tunnistamiseen tarvittava data välitetään maksujärjestelmään. Julkaisussa kuvatussa pankkipalvelussa asiakas asettaa pankin palvelukortin, joka sisältää SIM-yksikön, GSM-verkon päätelaitteeseen. Puhelinperustaisessa pankkipalvelussa päätelaite voi olla standardin mukainen GSM-matkaviestin. Julkaisussa kuvatulla menetelmällä voidaan käyttää langatonta tietoliikenneyhteyttä maksujen ja/tai laskujen tai muiden vastaavien pankkipalvelujen tai kassapalvelujen toteuttamiseen.

Ongelmana yllä mainituissa ratkaisuissa on, että niissä ei oteta kantaa maksun luotettavuuteen maksajan ja maksun saajan kannalta. Käytettäessä matkaviestintä maksamiseen on tärkeää, että sekä maksaja että maksun saaja voivat luottaa järjestelmään. Maksajan on tarkkaan tiedettävä, mistä maksaa, minkä verran maksaa, kenelle maksaa, miten maksaa jne. Maksun saajan on myös tarkkaan tiedettävä, kuka maksaa, mistä maksaa, minkä verran maksaa jne.

Kuten tiedetään, tiedon siirtäminen paikasta toiseen sähköisessä muodossa on helppoa. Sen sijaan vaikeampaa on varmistua siitä, että siirretty tieto säilyy siirron aikana muuttumattomana ja siitä, että esimerkiksi matkapuhelimen näytöllä esitetty tieto lähetetään juuri sellaisenaan ja muuttumattomana vastaanottajalle.

Entuudestaan on tunnettua käyttää tiivistettä, joka on lähetettävästä tiedosta muodostettu ja laskettu tietokenttä. Tiivisteen laskemiseen käytetään

yleensä algoritmia, joka on yksisuuntainen funktio eli tiivisteestä ei ole mahdollista selvittää sen muodostamiseen käytettyjä tietoja. Eräs käytettävä algoritmi voi olla SHA-1 (Secure Has Algorithm).

Digitaalisella allekirjoituksella, jota pidetään yleisenä vaatimustasona sähköisessä maksamisessa, varmistetaan välitettävän aineiston eheys ja lähettäjän alkuperä. Digitaalinen allekirjoitus muodostetaan salaamalla välitettävästä aineistosta laskettu tiiviste lähettäjän salaisella avaimella. Koska kukaan muu ei tunne lähettäjän salaista avainta, voi vastaanottaja purkaessaan salauksen lähettäjän julkista avainta käyttäen varmistua siitä, että aineisto on muuttumaton ja lähettäjän muodostama. Eräs esimerkki digitaalisessa allekirjoituksessa käytettävästä algoritmista on RSA-salausalgoritmi, joka on julkisen ja salaisen avaimen salausjärjestelmä ja jota käytetään myös viestien salaamiseen.

KEKSINNÖN TARKOITUS

Esillä olevan keksinnön tarkoituksena on poistaa edellä esitetyt ongelmat. Erityisesti esillä olevan keksinnön tarkoituksena on tuoda esiin uuden tyyppinen menetelmä ja järjestelmä lomakkeen tai muun vastaavan tiedon allekirjoittamiseksi matkaviestimellä. Tässä yhteydessä lomakkeella voidaan tarkoittaa monen tyyppistä ja -sisältöistä sähköisesti tulkittavissa olevaan viestiä, sanomaa tai tietorakennetta. Lomake voi olla olio- tai ohjelmisto-objekti -tyyppinen informaatio, jota voidaan käsitellä sähköisessä muodossa.

Edelleen keksinnön tarkoituksena on tuoda esiin yksinkertainen ja helposti nykytekniikkaan implementoitavissa oleva menetelmä kaupallisten transaktioiden, kuten laskun maksamisen ja pankkiasioinnin, toteuttamiseksi matkaviestimellä.

KEKSINNÖN KOHDE

Keksinnön kohteena on menetelmä sähköisessä muodossa olevan lomakkeen, joka määriteltiin yllä, digitaaliseksi allekirjoittamiseksi turvallisesti käyttäen matkaviestintä tai muuta vastaavaa ja siihen verrattavissa olevaa laitetta. Menetelmässä siirretään allekirjoitettava aineisto, joka voi käsittää ainakin lomakkeen, sen tunnisteen, jaetun datan, ja/tai lomakkeeseen lisätyt olennaiset tiedot, matkaviestimeen. Allekirjoitettava aineisto voidaan muodostaa myös lomakkeen tunnisteesta ja lomakkeeseen liittyvistä olennaisista tiedoista, esimerkiksi lomakkeen ollessa pankkisiirtolomake, voidaan aineisto muodostaa pankkisiirtolomakkeen tunnisteesta ja lomakkeen olennaisten kenttien tiedoista, kuten maksajasta, saajasta ja summasta.

Keksinnön mukaisesti lasketaan allekirjoitettavasta aineistosta ensimmäinen tiiviste edullisesti ennen aineiston siirtämistä matkaviestimeen. Tiiviste lisätään aineistoon siirrettäväksi, jolloin sitä voidaan käyttää apuna tarkistuksen suorittamisessa. Kun aineisto on siirretty matkaviestimeen, se allekirjoitetaan matkaviestimessä ja edelleen keksinnön mukaisesti allekirjoitetun ja siirretyn aineiston oikeellisuus ja vastaavuus varmistetaan vertaamalla allekirjoitettua tiivistettä ja aineistosta ennen allekirjoitusta laskettua tiivistettä keskenään. Allekirjoittaminen voidaan tehdä myös siten, että allekirjoitetaan sekä olennaiset tiedot ja tiiviste, jolloin varmistutaan vielä siitäkin, että matkaviestimellä allekirjoitettu aineisto vastaa allekirjoitettavaksi siirrettyä aineistoa.

Kun kysymyksessä on tietyn tyyppiset sovellukset, kuten maksusovellukset, voidaan matkaviestimeen siirretty aineisto siirtää myös toiselle osapuolelle, esimerkiksi pankille, joka voi laskea saamas-

taan aineistosta tiivisteen. Matkaviestimessä allekirjoitettu aineisto voidaan edelleen salata ja siirtää salattu ja allekirjoitettu aineisto matkaviestimestä myös toiselle osapuolelle. Toinen osapuoli purkaa salauksen, tarkistaa allekirjoituksen, laskee matkaviestimestä saamastaan aineistosta toisen tiivisteen ja vertaa tätä ensimmäiseen alkuperäisestä aineistosta laskemaansa tiivisteeseen. Jos toinen osapuoli hyväksyy digitaalisen allekirjoituksen ja jos ensimmäinen ja toinen tiiviste vastaavat toisiaan, pankki hyväksyy matkaviestimellä tehdyn allekirjoituksen. Kun pankki on hyväksynyt allekirjoituksen, se voi merkitä allekirjoitettuun ja purettuun aineistoon aikaleiman ja arkistoida aineiston allekirjoitustapahtuman.

Edellä on kuvattu menettely, jossa asiakas allekirjoittaa pankille pankilta saamansa lomakkeen. Asiakas tai matkaviestimen käyttäjä voi olla yhteydessä paikallisesti maksuautomaattiin tai vastaavaan, jolloin maksuautomaatti välittää asiakkaalle maksettavaksi ja hyväksyttäväksi tarkoitetun lomakkeen. Tällöin asiakas käy sanomavaihtoa maksuautomaatin kanssa paikallisesti ja maksuautomaatti välittää digitaaliset allekirjoitustiedot edelleen. Kuitenkin maksuautomaatti voi välittämästään liikenteestä päätellä asiakkaan hyväksyneen sille tarjotun palvelun ja maksulomakkeen. Tällöin automaatti voi palvella asiakasta tämän haluamalla ja maksamalla tavalla paikallisesti odottamatta välttämättä pankilta hyväksyntää siitä. Tilanne vastaa käytännössä normaalia käytäntöä, jossa esimerkiksi kaupan kassalla asiakas pankkikortillaan maksaa tuotteet tai palvelut, ja kauppa tarjoaa ne asiakkaalle varmistamatta maksun oikeellisuutta pankista.

Aineisto voidaan myös salata ennen sen siirtämistä matkaviestimeen, jolloin matkaviestimessä on purettava salaus ennen aineiston allekirjoittamista. Tällä voidaan varmistaa se, että vain haluttu matka-

viestin vastaanottaa siirrettävän aineiston ja taata tietojen turvallisuus.

Lomakkeen muodostamiseen voidaan käyttää ennalta sovittua tunnisteellista lomakepohjaa, viestirakennetta tai mitä tahansa muuta sanomarakennetta, johon täydennetään ennalta sovitut oleelliset tiedot ennen lomakkeen siirtämistä matkaviestimeen. Tiiviste voidaan laskea esimerkiksi hash-funktiolla. Viestin ja/tai lomakkeen allekirjoitukseen ja/tai salaukseen voidaan käyttää julkisen ja salaisen avaimen menetelmää.

Keksinnön eräässä edullisessa sovelluksessa esitetään aineisto ja/tai osa siitä matkaviestimessä ennen aineiston allekirjoittamista. Esimerkiksi voidaan esittää lomakkeessa olevat saaja-, maksaja- ja viitetiedot sekä maksettava summa. Myös on mahdollista vaatia matkaviestimen käynnistämistä allekirjoitusmoodissa ennen aineiston siirtämistä siihen. Tämä voi käytännössä tarkoittaa sitä, että matkaviestimeen on syötettävä toinen ennalta määrätty PIN-koodi, jolla matkaviestin on konfiguroitu käynnistymään ennalta määrätyssä allekirjoitusmoodissa. Voidaan käyttää siis eräänlaista paikallista autentikointia.

Keksinnön kohteena on myös järjestelmä sähköisessä muodossa olevan lomakkeen digitaaliseksi allekirjoittamiseksi turvallisesti matkaviestimellä. Järjestelmään kuuluu edullisesti maksuautomaatti ja siihen yhdistetyt välineet allekirjoitettavan aineiston, joka määriteltiin yllä, muodostamiseksi ja siirtämiseksi matkaviestimeen. Maksuautomaatilla voidaan tässä tarkoittaa mitä tahansa paikallista ja paikallisesti käytettävää automaattia, joka voi olla tietoliikenneverkon välityksellä yhdistetty palvelutarjoajaan, kuten pankkiin, kauppaan tai vastaavaan.

Maksuautomaatti voi olla toteutettu myös paikallisesti tietokoneeseen, joka on yhteydessä esimerkiksi Internet-verkon välityksellä palveluntarjoajaan,

jolloin palveluntarjoaja tarjoaa tuotteitaan ja palveluitaan Internet-verkon välityksellä. Tässä tapauksessa allekirjoitettava aineisto siirretään tietokoneelta allekirjoitettavaksi matkaviestimeen paikallista yhteyttä käyttäen tai suoraan palveluntarjoajan omalta palvelimelta käyttämättä paikallista tietokonetta ja yhteyttä.

Keksinnön mukaisesti maksuautomaattiin kuuluu välineet ensimmäisen tiivisteen laskemiseksi allekirjoitettavasta aineistosta. Samaten matkaviestimeen kuuluu allekirjoitusvälineet siihen siirretyn aineiston allekirjoittamiseksi. Allekirjoitusvälineisiin voi kuulua muisti, johon on tallennettu allekirjoituksen ja salauksen vaatimat algoritmit ja avaimet, ja prosessori, joka on yhdistetty muistiin ja joka käsittelee aineistoa toteuttaen digitaalisen allekirjoituksen ja mahdollisesti salauksen. Lisäksi maksuautomaattiin kuuluu välineet allekirjoitetun ja siirretyn aineiston oikeellisuuden varmistamiseksi vertaamalla matkaviestimessä allekirjoitettua tiivistettä ja aineistosta ennen allekirjoitusta laskettua tiivistettä keskenään.

Järjestelmään voi myös kuulua palvelin, joka on yhdistetty maksuautomaattiin ja/tai matkaviestimeen ja joka on toisen osapuolen, kuten pankin tai luottokorttiyhtiön, valvonnassa. Tällainen palvelin voi siis olla esimerkiksi pankin ylläpitämä ja sitä voidaan käyttää pankkitapahtumien toteuttamisessa. Palvelimeen voi myös kuulua välineet matkaviestimen tekemän digitaalisen allekirjoituksen oikeellisuuden todentamiseksi ja salaus- ja purkuvälineet palvelimen ja maksuautomaatin ja/tai matkaviestimen välillä siirrettävän aineiston salaamiseksi ja purkamiseksi.

Palvelimeen voi kuulua myös välineet aikaleiman merkitsemiseksi aineistoon ja välineet aineiston allekirjoitustapahtuman arkistoimiseksi sen jälkeen, kun allekirjoitus on todettu oikeaksi. Nämä voi-

daan toteuttaa ammattimiehen sinänsä tuntemalla tavalla, eikä niitä sen vuoksi kuvata tässä tarkemmin.

Esillä olevan keksinnön etuna tunnettuun tekniikkaan verrattuna on, että keksinnön ansiosta maksusovellusten, varmistustapahtumien ja muiden toteuttaminen matkaviestimellä tulee entistä helpommaksi. Keksinnön ansiosta matkaviestintä voidaan luotettavasti käyttää digitaalisessa allekirjoituksessa ja tällöin digitaalinen allekirjoitus voidaan yhdistää monen eri sovelluksen yhteyteen.

KUVALUETTELO

Seuraavassa keksintöä selostetaan edullisten sovellusesimerkkien avulla viittaamalla oheiseen piirustukseen, jossa:

kuvio 1 esittää erästä esillä olevan keksinnön mukaista edullista järjestelmää;

kuvio 2 esittää erästä toista esillä olevan keksinnön mukaista edullista järjestelmää;

kuvio 3 esittää vuokaaviomuodossa esillä olevan keksinnön erään edullisen sovelluksen; ja

kuvio 4 esittää kaaviomaisesti erään edullisen esimerkin allekirjoitettavan aineiston muodostamisesta esillä olevan keksinnön yhteydessä.

Kuviossa 1 esitettyyn järjestelmään kuuluu paikallinen maksuautomaatti (Local Payment Machine, LPM) 2 ja siihen yhdistetyt välineet allekirjoitettavan aineiston, käsittäen lomakkeen, sen tunnisteen, jaetun datan ja/tai siihen liitetyt olennaiset tiedot, muodostamiseksi. Lisäksi maksuautomaattiin kuuluu siihen yhdistetyt välineet 4 aineiston siirtämiseksi matkaviestimeen. Vastaavasti matkaviestimeen kuuluu välineet 1, joilla matkaviestin (MS) kommunikoi maksuautomaatin kanssa. Eräässä edullisessa sovelluksessa välineet 1 ja 4 on toteutettu Bluetooth-teknologiaa käyttäen. Tarkempaa kuvausta Bluetooth-tekniikasta esitetään esimerkiksi WWW-sivulla www.bluetooth.com. Myös

muita tunnettuja siirtoyhteyskäytäntöjä, kuten infrapunaliitäntää voidaan käyttää

Edelleen kuviossa 1 esitettyyn järjestelmään kuuluu palvelin 8, joka on yhdistetty TCP/IP-yhteydellä maksuautomaattiin 2 ja joka tässä esimerkissä on pankin hallinnoima. Palvelimeen kuuluu edelleen välineet 9 digitaalisen allekirjoituksen oikeellisuuden todentamiseksi - käytännössä niillä puretaan vastaanotetut salaviestit ja verrataan niissä olevia digitaalisia allekirjoituksia saatuihin käyttäjätietoihin. Lisäksi palvelimeen kuuluu välineet 11 ja 12, joilla merkitään aikaleima allekirjoitettuun aineistoon ja arkistoidaan allekirjoitustapahtuma sen jälkeen, kun allekirjoitus on todettu oikeaksi. Vastaavat todentamisvälineet voivat kuulua myös maksuautomaattiin ja tässä ne on merkitty numerolla 7. Välineillä 7, 11 ja 12 voi olla myös ominaisuus, jolla tarvittavat julkiset avaimet noudetaan esimerkiksi TCP/IP-verkon välityksellä yleisiltä avainhallintapalvelimilta.

Kuvion 1 esimerkissä siirretään salattu aineisto, johon kuuluu laskulomake ja laskulomakkeesta laskettu tiiviste H1 maksuautomaatilta 2 matkaviestimeen MS, vaihe 1. Matkaviestimessä aineisto eli laskulomake ja siihen tallennetut tiedot maksun saajasta, maksajasta, summasta ja maksun viitteestä esitetään matkapuhelimen näytöllä (10), josta matkaviestimen käyttäjä voi tarkistaa, mitä on allekirjoittamassa. Sen jälkeen käyttäjä allekirjoittaa matkaviestimellä MS aineiston ja siitä lasketun tiivisteen H1. Aineisto, johon on lisätty tiiviste $H1_{ds}$ allekirjoitettuna digitaalisesti siirretään maksuautomaattiin 2, vaihe 2. Maksuautomaatin 2 ja matkaviestimen MS välinen sanomaliikenne voidaan salata käyttäen matkaviestimen käyttäjän ja maksuautomaatin julkisia ja salaisia avaimia. Kun maksuautomaatissa 2 on tarkistettu allekirjoituksen oikeellisuus, lähetetään clearing-sanoma,

vaihe 3 maksuautomaatista edelleen pankkiin. Clearing on tunnettua ja yleisesti pankkimaailmassa käytettyä tekniikkaa eikä sitä kuvata tässä tarkemmin.

Seuraavaksi viitataan kuvioon 2, jossa on esitetty vastaavanlainen järjestelmä kuin kuviossa 1, mutta tässä järjestelmää käytetään hieman eri tavalla. Ensin maksuautomaatissa muodostettu aineisto, esimerkiksi lomake, siirretään pankkiin, vaihe 1. Sen jälkeen aineistosta lasketaan maksuautomaatissa tiiviste H1, joka siirretään matkaviestimeen allekirjoitettavaksi, vaihe 2. Siirto voidaan tehdä käyttäen paikallista esimerkiksi Bluetooth-yhteyttä. Matkaviestimessä saatu sanoma allekirjoitetaan digitaalisesti ja sen jälkeen allekirjoitettu ja mahdollisesti salattu aineisto lähetetään pankkiin, vaihe 3. Pankissa verrataan maksuautomaatilta saadusta aineistosta laskettua tiivistettä H1 matkaviestimeltä saatuun tiivisteeseen $H1_{ds}$, joka on digitaalisesti allekirjoitettu ja jos ne täsmäävät, hyväksytään allekirjoitustapahtuma. Tämän jälkeen palvelimella tehdään aikaleimaus ja arkistoidaan saatu allekirjoitustapahtuma. Pankki voi olla myös muu vastaava palveluntarjoaja, kuten luottokorttiyhtiö, jolloin edellä kuvatun lisäksi allekirjoituksen oikeellisuus vahvistetaan pankille, maksuautomaatille tai muulle palveluntarjoajalle. Tällöin luottokorttiyhtiö vahvistettuaan allekirjoituksen ottaa vastuun tapahtumasta.

Viitaten vielä kuvioon 3 esitetään eräs keksinnön edullinen sovellus. Aluksi muodostetaan aineisto, joka on tarkoitettu allekirjoitettavaksi matkaviestimellä, lohko 31. Aineistosta lasketaan ensimmäinen tiiviste, H1, lohko 32. Sen jälkeen tarkistetaan, lohko 45, onko aineisto salattava ennen lähetystä matkaviestimeen. Jos aineisto on salattava, siirrytään lohkoon 46 ja salataan se käyttäen matkaviestimen käyttäjän julkista avainta. Salauksen jälkeen siirrytään lohkoon 33. Jos aineistoa ei tarvitse salata,

siirrytään suoraan lohkoon 33, jossa aineisto siirretään matkaviestimelle. Seuraavaksi siirrytään lohkoon 34 ja tarkistetaan matkaviestimen näytöllä esitettävä aineisto tai sen olennaiset tiedot eli esimerkiksi laskun saajan ja maksun oikeellisuus. Jos maksaja hyväksyy, lohkossa 35, siirrytään lohkoon 37 ja allekirjoitetaan aineisto. Jos maksaja ei hyväksy lohkossa 35, siirrytään lohkoon 36, jossa lähetetään hylkäyssanoma aineiston lähettäjälle, esimerkiksi maksuautomaatille ja lopetetaan prosessi. Lohkosta 37 siirrytään lohkoon 38, jossa muodostetaan aineisto digitaalisesta allekirjoituksesta ja tiivisteestä ja mahdollisesti saadusta aineistosta, johon kuuluu esimerkiksi lomakkeen olennaiset tiedot, lohko 38. Sen jälkeen aineisto siirretään maksuautomaattiin, lohko 39, josta edelleen siirrytään lohkoon 40 ja verrataan siirretystä aineistosta laskettua tiivistettä allekirjoitettuun tiivisteeseen. Jos tiivisteet vastaavat toisiaan, lohko 41, hyväksytään allekirjoitus ja tehdään seuraavaksi määritellyt toimenpiteet.

Jos lohkossa 40 tiivisteet eivät täsmänneet, voidaan proseduuri toistaa. Tässä vaiheessa on mahdollista käyttää laskuria, jolla tarkkaillaan sitä, ettei aineistoa lähetetä useammin kuin ennalta on sovittu. Lohkosta 40 siirrytään lohkoon 43, jossa kasvatetaan laskurin k = k+1 arvoa yhdellä ja siitä edelleen siirrytään lohkoon 44, jossa tarkistetaan laskurin arvo eli se, montako kertaa aineisto on siirretty matkaviestimeen. Jos arvo ylittää ennalta sovitun, siirrytään lohkoon 42 ja lähetetään hylkäyssanoma matkaviestimeen. Jos laskurin arvo on pienempi kuin ennalta sovittu, siirrytään uudelleen lohkoon 31 ja toistetaan prosessi.

Kuviossa 4 on esitetty eräs edullinen tapa muodostaa ja allekirjoittaa lomake tai aineisto digitaalisesti. Matkaviestimeen siirrettävään aineistoon kuuluu lomaketunniste, joka on yksilöllinen kaikille

käytettäville lomakkeille, lohko 51. Lomaketunnisteeseen liittyy lomakekaavain, lohko 52, joiden perusteella sovellukset, asiakas ja sovelluksen tarjoaja tietävät tarkalleen, millaisesta lomakkeesta on kysymys. Aineistoa muodostettaessa lomaketunniste ja lomakekaavain ketjutetaan peräkkäin, kuten kuviossa 4 on esitetty ja sen jälkeen niistä lasketaan ensimmäinen tiiviste, lohko 54.

Lomakkeeseen liitetään usein lomakedataa, lohko 53, jo ennen sen siirtämiseksi matkaviestimeen allekirjoitettavaksi. Tällöin lomaketunniste ja lomakedata ketjutetaan peräkkäin kuvion 4 osoittamassa järjestyksessä ja niistä saatu bittijono edelleen ketjutetaan satunnaisten 16 tavun, lohko 55 kanssa. Niihin yhdistetään ensimmäinen tiiviste lohkosta 54.

Tässä vaiheessa aineisto on valmis siirrettäväksi matkaviestimeen, minkä jälkeen siitä lasketaan toinen tiiviste, lohko 56. Käytännössä toinen tiiviste lasketaan matkaviestimessä ja lisätään allekirjoitettavaan sanomaan, lohko 57. Samaten allekirjoitettavaan sanomaan on lisätty käyttäjädata, jota matkaviestimen käyttäjä on voinut täydentää omilla tiedoillaan tarpeen mukaan. Edullisesti myös tähän allekirjoitettavaan viestiin lisätään lohkosta 55 16 satunnaistavua, jolloin aineiston siirtäjän ja matkaviestimen käyttäjän muodostaman allekirjoitetun sanoman oikeellisuutta voidaan tarkistaa. Kun satunnaistavut käyttäjädata ja toinen tiiviste on asetettu peräkkäin, käyttäjän matkaviestimessä allekirjoitetaan sanoma digitaalisesti. Tämän jälkeen sanoma voidaan välittää eteenpäin toiselle osapuolelle, maksuautomaattiin tai muulle aineiston alkuperälähteelle.

Yhteenvetona todetaan vielä, että keksintönä on toteuttaa menetelmä ja järjestelmä, jossa käyttäjä, palvelun tarjoaja ja pankki, jotka mainitaan esimerkkinä, voivat varmistua digitaalisen allekirjoituksen oikeellisuudesta. Tarkoituksena on, että allekirjoi-

tettava aineisto voidaan sitoa johonkin käyttäjän dataan, formaattiin ja käyttäjän tekemään digitaaliseen allekirjoitukseen. Allekirjoitus on siis pystyttävä sitomaan tietynlaiseen ketjuun, joka käytännössä vastaa nykyisin käytössä olevaa ketjua, jossa käyttäjä omalla manuaalisella allekirjoituksellaan hyväksyy ostoksiaan. Samaten menetelmän tarkoituksena on identifioida allekirjoittaja luotettavasti ja lainsäätäjän vaatimalla ja tarkoittamalla tavalla.

Esillä olevaa keksintöä ei rajata tässä esitettyihin esimerkkeihin, vaan monet muunnokset ovat mahdollisia pysyttäessä oheisten patenttivaatimusten määrittelemän suojapiirin rajoissa.

PATENTTIVAATIMUKSET

1. Menetelmä sähköisessä muodossa olevan lomakkeen digitaaliseksi allekirjoittamiseksi turvallisesti matkaviestimellä, johon menetelmään kuuluu vaiheet

siirretään allekirjoitettava aineisto, johon kuuluu lomake, sen tunniste, jaettu data, ja/tai siihen lisätyt olennaiset tiedot, matkaviestimeen, t u n n e t t u siitä, että

lasketaan allekirjoitettavasta aineistosta ensimmäinen tiiviste (H1);

lisätään tiiviste aineistoon siirrettäväksi matkaviestimeen;

allekirjoitetaan digitaalisesti matkaviestimellä siihen siirretty aineisto; ja

varmistetaan allekirjoitetun ja siirretyn aineiston oikeellisuus vertaamalla allekirjoitettua tiivistettä ja aineistosta ennen allekirjoitusta laskettua tiivistettä keskenään.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että

siirretään matkaviestimeen allekirjoitettavaksi siirretty aineisto toiselle osapuolelle; ja

allekirjoitettu aineisto toiselle osapuolelle, jolloin toinen osapuoli varmistaa allekirjoituksen oikeellisuuden.

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, t u n n e t t u siitä, että salataan aineisto ennen sen siirtämistä matkaviestimen ja toisen osapuolen välillä; ja

puretaan salaus ennen aineiston käsittelyä, kuten allekirjoitusta ja oikeellisuuden varmistamista.

4. Jonkin edeltävistä patenttivaatimuksista 1 - 3 mukainen menetelmä, t u n n e t t u siitä, että

käytetään lomakkeen muodostamiseen ennalta sovittua tunnisteellista lomakepohjaa, johon täydennetään

oleelliset tiedot ennen sen siirtämistä matkaviestimeen.

5. Jonkin edeltävistä patenttivaatimuksista 1 - 4 mukainen menetelmä, t u n n e t t u siitä, että muodostetaan tiiviste hash-funktiolla.

6. Jonkin edeltävistä patenttivaatimuksista 1 - 5 mukainen menetelmä, t u n n e t t u siitä, että käytetään viestin allekirjoitukseen ja/tai salaukseen julkisen ja salaisen avaimen menetelmää.

7. Jonkin edeltävistä patenttivaatimuksista 1 - 6 mukainen menetelmä, t u n n e t t u siitä, että esitetään aineisto ja/tai osa siitä matkaviestimessä ennen aineiston allekirjoittamista.

8. Jonkin edeltävistä patenttivaatimuksista 1 - 7 mukainen menetelmä, t u n n e t t u siitä, että käynnistetään matkaviestin allekirjoitusmoodissa ennen aineiston siirtämistä matkaviestimeen.

9. Jonkin edeltävistä patenttivaatimuksista 1 - 8 mukainen menetelmä, t u n n e t t u siitä, että merkitään aineistoon aikaleima; ja arkistoidaan aineiston allekirjoitustapahtuma sen jälkeen, kun allekirjoitus on todettu oikeaksi.

10. Järjestelmä sähköisessä muodossa olevan lomakkeen digitaaliseksi allekirjoittamiseksi turvallisesti matkaviestimellä (MS), johon järjestelmään kuuluu

maksuautomaatti (2);

maksuautomaattiin yhdistetyt välineet (3) allekirjoitettavan aineiston, johon kuuluu lomake, sen tunniste, jaettu data, ja/tai siihen lisätyt olennaiset tiedot, muodostamiseksi; ja

maksuautomaattiin yhdistetyt välineet (4) aineiston siirtämiseksi matkaviestimeen (MS), t u n n e t t u siitä, että

maksuautomaattiin kuuluu välineet (5) ensimmäisen tiivisteen (H1) laskemiseksi allekirjoitettavasta aineistosta;

matkaviestimeen kuuluu allekirjoitusvälineet (6) siihen siirretyn aineiston allekirjoittamiseksi; ja

maksuautomaattiin kuuluu välineet (7) allekirjoitetun ja siirretyn aineiston oikeellisuuden varmistamiseksi vertaamalla allekirjoitettua tiivistettä($H1_{ds}$) ja aineistosta ennen allekirjoitusta laskettua tiivistettä (H1) keskenään.

11. Patenttivaatimuksen 10 mukainen järjestelmä, t u n n e t t u siitä, että järjestelmään kuuluu

palvelin (8), joka on yhdistetty maksuautomaattiin (2) ja matkaviestimeen (MS) ja kolmannen osapuolen valvonnassa; ja

matkaviestimeen kuuluu välineet allekirjoitetun aineiston salaamiseksi.

12. Patenttivaatimuksen 10 tai 11 mukainen järjestelmä, t u n n e t t u siitä, että palvelimeen (8) kuuluu

välineet (9) digitaalisen allekirjoituksen oikeellisuuden todentamiseksi.

13. Jonkin edeltävistä patenttivaatimuksista 10 - 12 mukainen menetelmä, t u n n e t t u siitä, että matkaviestimeen kuuluu

välineet (10) aineiston ja/tai osan siitä esittämiseksi matkaviestimessä ennen aineiston allekirjoittamista.

14. Jonkin edeltävistä patenttivaatimuksista 10 - 13 mukainen menetelmä, t u n n e t t u siitä, että palvelimeen (8) kuuluu

välineet (11) aikaleiman merkitsemiseksi aineistoon; ja

välineet (12) aineiston allekirjoitustapahtuman arkistoimiseksi sen jälkeen, kun allekirjoitus on todettu oikeaksi.

(57) TIIVISTELMÄ

Menetelmä sähköisessä muodossa olevan lomakkeen digitaaliseksi allekirjoittamiseksi turvallisesti matkaviestimellä. Menetelmässä siirretään allekirjoitettava aineisto, johon kuuluu lomake, sen tunniste, jaettu data, ja/tai siihen lisätyt olennaiset tiedot, matkaviestimeen, lasketaan allekirjoitettavasta aineistosta ensimmäinen tiiviste (H1), lisätään tiiviste aineistoon siirrettäväksi matkaviestimeen, allekirjoitetaan digitaalisesti matkaviestimellä siihen siirretty aineisto ja varmistetaan allekirjoitetun ja siirretyn aineiston oikeellisuus vertaamalla allekirjoitettua tiivistettä ja aineistosta ennen allekirjoitusta laskettua tiivistettä keskenään. Keksinnön ansiosta matkaviestintä voidaan turvallisesti käyttää digitaaliseen allekirjoitukseen erilaisissa sovelluksissa.

(Fig. 1)